Hrsg. Markus Beckedahl und Andre Meister

Überwachtes Netz

Edward Snowden und der größte Überwachungsskandal der Geschichte





Hrsg. Markus Beckedahl und Andre Meister

Überwachtes Netz

Edward Snowden und der größte Überwachungsskandal der Geschichte





Hrsg. Markus Beckedahl, Andre Meister

Überwachtes Netz

Edward Snowden und der größte Überwachungsskandal der Geschichte

Impressum

Überwachte Welt – Edward Snowden und der größte Überwachungsskandal der Geschichte

Herausgeber: Markus Beckedahl, Andre Meister
Redaktion: Jan-Peter Kleinhans, Anna Biselli, Kilian Froitzhuber, Nicolas Fennen, Andrea, Markus Beckedahl, Andre Meister, Matthias »wetterfrosch« Mehldau

Titelbild: Laura Poitras / Praxis Films; 3.0, Komplette Lizenz: https://creativecommons.org/licenses/by/3.0/
Montage: Jan-Peter Kleinhans, »wetterfrosch«

Satz: »wetterfrosch«
Verlag: newthinking communications, Berlin, in Kooperation mit epubli GmbH, Berlin

ISBN: 978-3-8442-7366-3
URL: http://netzpolitik.org/ueberwachtes-netz/



Inhaltsverzeichnis

Dank

Als erstes möchten wir uns bei Edward Snowden bedanken. Er riskiert sein Leben, um mit Mut und Zivilcourage den größten Überwachungsskandal in der Geschichte der Menschheit aufzudecken. Ebenfalls möchten wir uns bei seinen journalistischen Partnern wie Glenn Greenwald und Laura Poitras und allen anderen bedanken, die mithelfen, diesen Skandal zu dokumentieren und an die Öffentlichkeit zu bringen.

Dieses Buch wäre nicht ohne die Mithilfe zahlreicher Menschen möglich geworden. Wir möchten allen Autorinnen und Autoren dafür danken, uns bereits veröffentlichte Texte geschenkt oder sogar extra für dieses Buch geschrieben zu haben. Wir waren angenehm überrascht, dass wir so viel positives Feedback auf das Projekt erhalten haben.

Die Realisierung wäre nicht ohne ein großes Team im Hintergrund möglich gewesen. Wir möchten uns bei Jan-Peter Kleinhans für viel Unterstützung bei der Koordinierung, Übersetzung und Lektorat sowie Matthias »wetterfrosch« Mehldau für alle Fragen rund um das Design und Layout bedanken.

Zahlreiche Texte mussten vom Englischen übersetzt, andere Texte redigiert werden. Das verdanken wir vor allem Anna Biselli, Kilian Froitzhuber, Nicolas Fennen, Andrea, Caroline Kleine (Lesart), Eva und Jens. Wir danken auch allen Kommentatoren, die uns Vorschläge für einen Titel gemacht haben.

Und ohne das Team von newthinking wäre es uns auch nicht möglich gewesen, so viel Zeit in das Projekt zu stecken. Das Zusammenstellen dieses Buches war auch ein Experiment, wie man selbst ein Buch verlegen kann und ob man trotz des zeitgleichen Verschenken überhaupt Geld verdienen kann. Zuerst sollte das Buch nur digital erscheinen. Wir freuen uns, mit epubli einen Partner gefunden zu haben, , der uns ermöglicht, das Buch nach eigenen Vorstellungen und mit großer Gewinnbeteiligung zu drucken. Auch in digitalen Zeiten

freuen wir uns darauf, die Arbeit von Monaten gedruckt in Händen halten zu können.

Auch wenn wir daran kein Geld verdienen sollten, um unsere Redaktion zu refinanzieren, hat sich die Erfahrung bereits ausgezahlt. Vor allem war unsere größte Motivation, die Debatte um diesen größten Überwachungsskandal der Menschheit um Analysen und Reflexionen zu erweitern und vor allem konkrete Schritte in die Debatte zu bringen, wie wir Geheimdienste besser kontrollieren und unsere Privatsphäre sowie ein offenes Netz zurück erobern können.

Zum Schluß ein großer Dank an Alle, die sich für den Erhalt und Ausbau von Grundrechten sowie die ausufernde Überwachung engagieren und/oder dagegen anschreiben. Mit diesem Buch wollen wir auch dazu motivieren, einen langen Atem zu haben, um gemeinsam die Welt verändern zu können und unsere Freiheit zu erhalten. Es ist unser Netz und unsere Freiheit.

Dieses Buch erscheint unter einer freien Lizenz und kann gerne weiterkopiert werden. Wir freuen uns immer über finanzielle Unterstützung, um weiterhin unabhängig Projekte wie netzpolitik.org oder dieses Buch auf die Beine zu stellen und über Grundrechte in der digitalen Gesellschaft aufklären zu können. Unser gemeinnütziger Verein netzpolitik.org e.V. nimmt gerne Spenden entgegen:

Inhaber: netzpolitik.org e. V. (gemeinnützig)
Konto: 1149278400
BLZ: 43060967 (GLS Bank)
IBAN: DE62430609671149278400
BIC: GENODEM1GLS
Zweck: Spende netzpolitik.org

Vorwort

> *»Ich möchte nicht in einer Welt leben, in der alles, was ich sage, alles, was ich tue, aufgezeichnet wird. Das ist nichts, was ich bereit bin zu unterstützen. Das ist nichts, unter dem ich zu leben bereit bin.«*
>
> *– Edward Snowden im Interview mit dem Guardian, 10. Juni 2013*

Edward Snowden hat die größte Überwachungsmaschinerie der Menschheitsgeschichte enthüllt. Und täglich kommen neue Puzzlestücke ans Licht. Die Geheimdienste der westlichen Welt, allen voran die amerikanische NSA und das britische GCHQ, »versuchen sämtliche Formen der menschlichen Kommunikation zu sammeln, zu überwachen und zu speichern«, so der investigative Journalist Glenn Greenwald. Full Take.

Dabei geht es nicht um Terrorismus, womit dieser Überwachungs-Koloss in der Öffentlichkeit immer wieder gerechtfertigt wird. Die Dienste geben ganz offiziell selbst zu, dass die damit klassische Spionage betreiben – für Politik und Wirtschaft. Anders sind Wanzen in EU-Einrichtungen, das abgehörte Merkel-Telefon und gehackte Firmen-Netze auch nicht zu erklären. Schließlich nutzen die mächtigen, intransparenten und demokratisch nicht kontrollierbaren Geheimdienste ihren Datenschatz auch zum Erhalt der eigenen Macht. Der »Staat im Staat« existiert nicht nur in der Türkei, die Dienste führen ein Eigenleben.

Dabei kann eine Demokratie ohne Privatsphäre nicht funktionieren. Menschen brauchen einen »Kernbereich privater Lebensführung« zum Rückzug, zur Entwicklung und zur Reflexion. Stattdessen gibt es keine unbeobachtete Kommunikation mehr. Durch die Digitalisierung wird jede kleine Handlung von Computern verarbeitet – und damit von den Geheimdiensten abgeschnorchelt: Einkäufe, Reisen, Zahlungen, bald auch Zähneputzen und Autofahren. Und natürlich sämtliche Kommunikation und Interaktion. Das bedroht die Demokratie im Kern.

Vor zehn Jahren wurde netzpolitik.org gestartet, unter anderem als Reaktion auf den Geheimdienst-Skandal der damaligen Zeit: das

weltweite Spionagenetz Echelon. Alle unsere Befürchtungen wurden 2001 ganz offiziell vom Europaparlament bestätigt. Das war zwei Monate vor 9-11. Heute ist Echelon »ein Kinderspiel im Vergleich zur aktuellen Überwachung«.

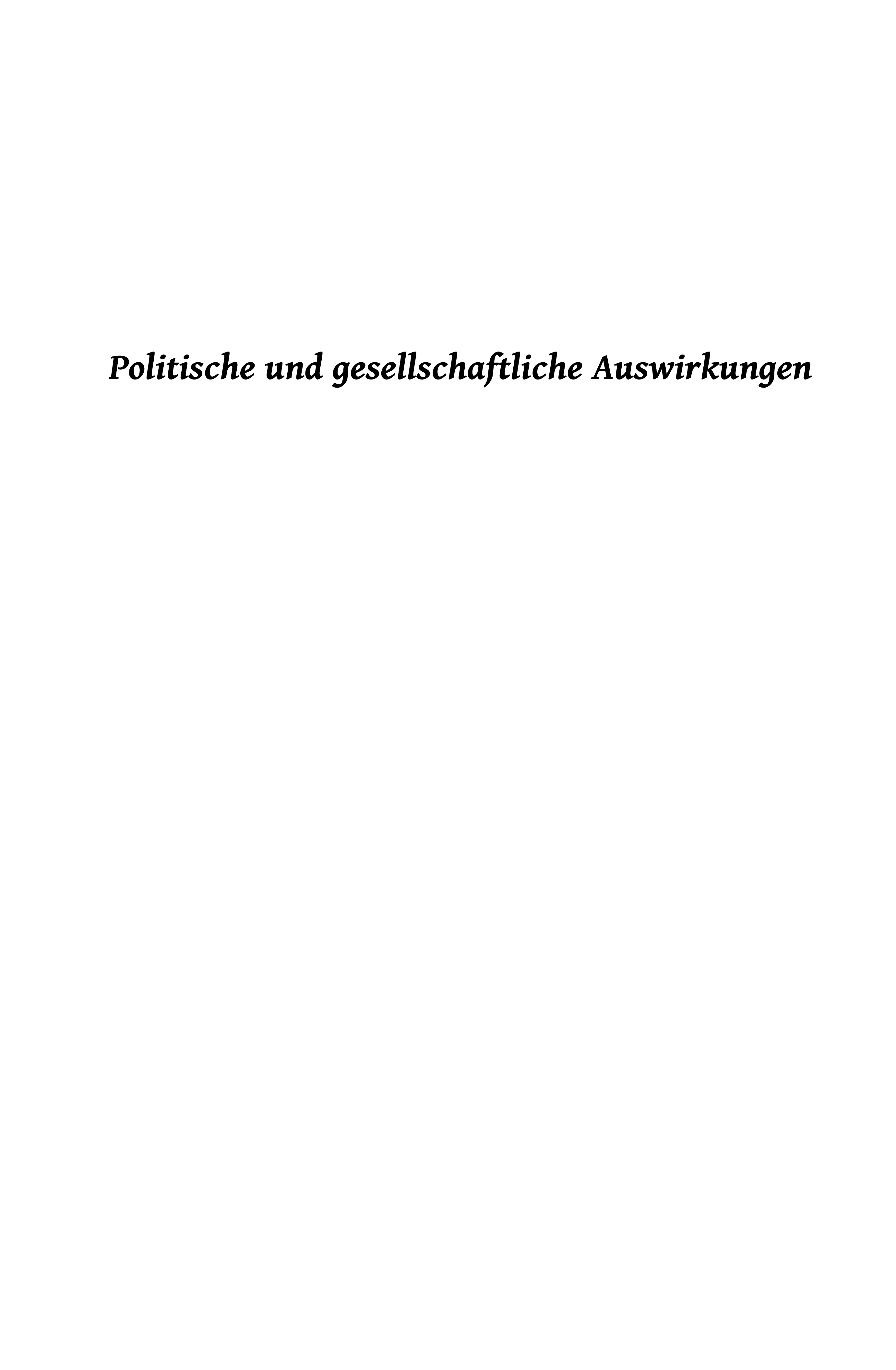
Wir wollen das nicht akzeptieren. Wir wollen den Kopf nicht in den Sand stecken und akzeptieren, dass wir mit dieser Überwachung leben müssen. Wie es unsere Regierungen wollen. Wir wollen unser Verhalten nicht umstellen, um damit umzugehen. Wir müssen die Überwachungsmaschinerie zurückdrängen und sehen Ansatzpunkte in einer Kombination aus technischen und politischen Mitteln.

Wir wissen, dass es vielen so geht. Wir haben in den vergangenen Monaten eine Vielzahl an Autorinnen und Autoren eingeladen, ihre Sicht auf die durch Edward Snowden ausgelösten Entwicklungen zu reflektieren und zu überlegen, welche Schlüsse aus den enthüllten Fakten zu ziehen sind.

Die Debatte darum darf nicht verstummen. Auf dem Spiel stehen Freiheit und Demokratie. Deswegen gibt es dieses Buch.

– Markus Beckedahl und Andre Meister

> *»Die gute Nachricht ist: Wir sind nicht paranoid.*
> *Die schlechte Nachricht ist: Wir werden alle überwacht.*
> *Jederzeit und überall.«*



Politische und gesellschaftliche Auswirkungen

Snowdens Rede zum Whistleblower-Award

Edward J. Snowden

Auf der Verleihung des Whistleblower-Awards am 30.08.2013 in Berlin, hielt Jacob Appelbaum stellvertretend für den leider abwesenden Edward Snowden eine Dankesrede[1]*. Mit freundlicher Unterstützung von Jacob Appelbaum können wir die Dankesrede von Edward Snowden abdrucken.*

Es ist eine große Ehre, dass mein Whistleblowing als Beitrag zum Allgemeinwohl wahrgenommen wird. Doch die größere Anerkennung und Aufmerksamkeit gebührt jenen Einzelpersonen und Organisationen in unzähligen Ländern auf der ganzen Welt, die sprachliche und geografische Grenzen gesprengt haben, um gemeinsam das öffentliche Recht auf Information und den Wert der Privatsphäre zu verteidigen.

Es bin nicht nur ich, sondern die Allgemeinheit, die von dieser mächtigen Wandlung hin zu der Abschaffung unserer Grundrechte betroffen ist. Es bin nicht nur ich, sondern Zeitungen aus aller Welt, die Gründe haben, unsere Regierungen dafür verantwortlich zu machen, wenn mächtige öffentliche Vertreter versuchen, solche Themen durch Gerüchte und Anschuldigungen kleinzureden. Und es bin nicht nur ich, sondern ganz gewiss auch mutige Regierungsvertreter in der ganzen Welt, die neue Schutzmaßnahmen und Limitierungen vorschlagen, um zukünftige Angriffe auf unser aller Rechte und unser Privatleben zu verhindern.

Ich danke all jenen, die sich an ihre Freunde und Familien gewandt haben, um ihnen zu erklären, warum sie anlasslose Überwachung etwas angeht. Sie trifft den Mann, der an einem heißen Tag eine Sturmmaske trägt, sie trifft die Frau mit einem Schild und einem Schirm im Regen, sie trifft den jungen Studenten, auf dessen Laptop sich Sticker zu Freiheitsrechten befinden und den Gymnasiasten, der sich in der letzten Reihe des Klassenraums Internet-Memes ausdenkt.

All diese Menschen verstehen, dass eine Veränderung mit einer einzelnen Äußerung beginnt und sie haben der Welt eine Botschaft überbracht. Regierungen müssen sich uns gegenüber für ihre Entscheidungen rechtfertigen – denn es sind Entscheidungen über die Welt, in der wir alle leben. Die Entscheidungen über Rechte und Freiheiten von Menschen sind Sache der Allgemeinheit und dürfen nicht der Geheimhaltung durch Regierungen unterliegen.

Diese Freude wird für mich jedoch von dem Bewusstsein überschattet, was uns heute hier zusammengebracht hat. Im Amerika der heutigen Zeit hat die Kombination aus schwachem Rechtsschutz von Whistleblowern, schlechten Gesetzen zur Verteidigung öffentlicher Interessen und zweifelhafter Immunität derjenigen, die sich abseits von Gesetzen bewegt haben, zur Pervertierung des Systems aus Anreizen geführt, das Geheimhaltung und Regierung reguliert. Ergebnis dessen ist eine Situation, die einen unzumutbaren Preis für die Bewahrung der Grundpfeiler einer freiheitlichen Demokratie – informierte Bürger – fordert.

Den Mächtigen gegenüber die Wahrheit auszusprechen, haben Whistleblower mit ihren Freiheiten, Familien und ihrer Heimat bezahlt.

Von diesem Zustand profitieren weder Amerika noch der Rest der Welt. Es braucht keine besondere Expertise, um zu verstehen, dass es zu Unwissenheit und Verunsicherung führt, wenn notwendige Warnrufe mit der Bedrohung nationaler Sicherheit gleichgesetzt werden. Eine Gesellschaft, die dem Irrtum einer Volksweisheit erliegt, man müsse »den Überbringer schlechter Nachrichten erschießen«, wird schnell merken, dass bald nicht nur die Überbringer, sondern auch alle anderen Nachrichten ausbleiben. Es ist richtig, den Sinn einer solchen Politik und ihre unbeabsichtigten Konsequenzen in Frage zu stellen.

Wenn die Strafe für die böswillige Übergabe von Geheiminformationen an fremde Regierungen geringer ist, als wenn diese Informationen mit guten Absichten an die Öffentlichkeit gegeben werden, ermutigen wir damit nicht Spione viel mehr als Whistleblower? Was bedeutet es für die

Allgemeinheit, wenn Anti-Terror-Gesetze auf den Journalismus angewendet werden?

Können wir in einer offenen Gesellschaft leben, wenn wir Einschüchterung und Vergeltung über Recherche und die Suche nach Wahrheit stellen?

Wo ziehen wir die Grenze zwischen nationaler Sicherheit und öffentlichem Interesse?

Wie können wir auf die Angemessenheit dieser Grenze vertrauen, wenn diejenigen, die sie festlegen, ausschließlich aus Reihen der Regierung stammen?

Fragen wie diese können nur durch eine öffentliche Diskussion wie die heutige beantwortet werden. Wir dürfen niemals vergessen, was die Geschichte uns über die Konsequenzen übermächtiger Überwachung gelehrt hat. Aber genauso wenig dürfen wir unsere Macht aus den Augen verlieren, diese Systeme in unser aller Interesse zu verändern.

Unser Weg war und ist steinig, aber er führt uns zu besseren Zeiten. Zusammen können wir die Sicherheit und die Rechte der kommenden Generationen sichern.

All jenen, die an dieser Diskussion teilhatten, vom höchsten offiziellen Repräsentanten bis zum kleinen Bürger, sage ich: Danke.

Asyl für Snowden

Markus Beckedahl

»Es ist gefährlich, Recht zu haben, wenn die Regierung Unrecht hat.« Was dem politisch verfolgten NSA-Whistleblower Edward Snowden derzeit widerfährt, wusste schon Voltaire in Worte zu packen. Der 30-jährige Systemadministrator hat der Weltöffentlichkeit einen Dienst erwiesen, in dem er mit einer Serie interner Dokumente bewiesen hat, was bisher oft als Verschwörungstheorie abgetan wurde. Täglich kommen neue Details des größten Überwachungsskandals in der Geschichte der Menschheit an die Öffentlichkeit, ein Ende ist noch nicht absehbar. Mehrere Geheimdienste der Welt, in diesem Fall vor allem die der USA und Großbritannien, überwachen und speichern große Teile der weltweiten Kommunikation - unrechtmäßig auch in unserem Land. Verbindungsdaten und Inhalte aller Internet- und Telefon-Nutzer werden in riesigen Datenzentren für unbestimmte Zeit gespeichert und mit Algorithmen gerastert. Keine Datenschutzbehörde kontrolliert dies. Unsere Spitzenpolitiker erfahren davon aus der Zeitung. Dass auch diplomatische Vertretungen, Unternehmen und unsere Spitzenpolitiker betroffen sind, beweist, dass der Kampf gegen den Terror dabei nur eine Ausrede ist.

Edward Snowden ist damit ein klassischer Whistleblower: er hat Missstände an die Öffentlichkeit gebracht, die diese wissen sollte. Denn ohne informiert zu sein, können Gesellschaften auch nicht zustimmen oder kontrollieren, was in ihrem Namen mit ihren Daten gemacht wird. Spätestens durch die Berichte über das Ausspionieren diplomatischer Vertretungen und des Telefons von Angela Merkel wahrt Snowden damit auch die »politischen Interessen der Bundesrepublik Deutschland«. Das im Übrigen die Formulierung des Aufenthaltsgesetzes ist, wann eine Aufnahme von Asylsuchenden aus dem Ausland geboten ist.

Innen- und Außenpolitiker der Volksparteien begründen die mögliche Ablehnung eines Asylantrages von Edward Snowden in Deutschland

damit, dass die USA ein Rechtsstaat sind. Die Behandlung von Chelsea Manning, inklusive Folter und drohender Todesstrafe für das Aufdecken von Kriegsverbrechen, konterkarieren dieses Argument. Edward Snowden hätte momentan keine Chance auf einen fairen Prozess in den USA und würde im Gefängnis ruhig gestellt. Aber auch wenn es keinen Asylantrag gibt, hätte die Bundesregierung die Chance, Edward Snowden in ein Zeugenschutzprogramm zu stecken. Er ist der wichtigste Zeuge bei der Aufklärung dieses Überwachungsskandals.

Es ist unvorstellbar, dass ein chinesischer Geheimdienstler mit Informationen über die Hacking-Programme der Volksrepublik oder ein iranischer Wissenschaftler mit Informationen über das Atomprogramm der Islamischen Republik von den USA in sein Heimatland ausgeliefert würde. Die Ablehnung der Bundesregierung beweist damit bestenfalls ihre Doppelmoral, aber noch wahrscheinlich ihr Einverständnis mit dem umfangreichsten Überwachungsprogramm der Menschheitsgeschichte. Die Frage nach Snowdens Asylantrag ist eine politische Frage, die eine politische Antwort verlangt. Und die kann nur lauten: Asyl für Snowden!

Leben im Überwachungsstaat

Oder warum wir das dunkle Monster in unserer Mitte nicht länger ignorieren dürfen

Kai Biermann

Ich komme aus einem Land, das heute als der Inbegriff des Überwachungsstaates gilt. Für die Überwacher hatten wir damals viele Namen. Sie wurden »Horch und Guck« genannt, oder »die Firma«, meistens aber mit der Abkürzung bezeichnet, die bis heute jedem ein Begriff ist: »Stasi«. Das Ministerium für Staatssicherheit hatte so viele Angestellte, dass pro 180 Einwohner ein hauptamtlicher Mitarbeiter existierte. In keinem Land davor und in keinem danach kamen so viele Bewacher auf so wenige Überwachte, es war der größte Geheimdienstapparat der Weltgeschichte.

Die Stasi gehörte zum Alltag in der DDR. Niemand redete offen über sie, aber jeder wusste von ihr und jeder fürchtete sie. Die Warnung meiner Eltern, »das darfst du aber niemandem erzählen«, war in meiner Kindheit ein ständiger Begleiter. Meine Eltern hatten Angst, also hatte ich sie auch.

Trotzdem lebten alle irgendwie vor sich hin und versuchten, dieses Monstrum zu ignorieren, so gut es eben ging. Möglich war das durchaus, kaum jemand kannte Opfer des Terrors persönlich. Entweder waren die in den Westen abgeschoben worden, oder sie hielten wohlweislich die Klappe, um nicht wieder abgeholt zu werden. Das Dunkle ließ sich ganz gut verdrängen.

Selbst im Herbst 1989 ging das noch. Dabei wurden bei den Montagsdemos nicht mehr nur Einzelne abgeholt. Zu Hunderten verhaftete die Stasi nun Demonstranten, jede Woche, wahllos. Und die, die anschließend wieder freikamen, wollten nicht mehr schweigen, sie fertigten Gedächtnisprotokolle über ihre Erlebnisse, sie redeten. Plötzlich bekam die Stasi ein hässliches Gesicht, plötzlich war sie keine vage Ahnung mehr, kein Gerücht, keine Verschwörungstheorie – sie

wurde real, ihre Verhöre, ihre Drohungen, die Bedrohung, die von ihr ausging, wurde auf einmal jenen Menschen bewusst, die sie sehen wollten.

Noch immer aber konnte, wer wollte, das Monster beiseite schieben. Schließlich traf es nur die, die sich gegen den Staat auflehnten, die demonstrierten, Flugblätter druckten. Wer nicht aufmuckte, der hatte doch nichts zu befürchten, oder? Wie die Punkband Feeling B so richtig sang: »Wir woll'n immer artig sein, denn nur so hat man uns gerne.«

Der wahre Schrecken folgte erst später. Im Dezember 1991 trat das Stasi-Unterlagen-Gesetz in Kraft, die Opfer konnten nun nachlesen, was die Täter über sie gesammelt hatten. Meine Eltern beantragten sofort Einsicht in ihre Stasi-Akten. Es war ein Schock. In der kalten Sprache von Bürokraten wurde dort über Menschen geschrieben, die bereits verurteilt waren, obwohl noch nicht einmal eine Anklage existierte, geschweige denn irgendwelche Beweise.

Es war ein Schock, den wohl alle erlebten, die ihre Akten lasen. Denn plötzlich zeigte sich, dass jeder ein Staatsfeind gewesen sein konnte, auch wenn er selbst geglaubt hatte, dass er immer artig war. Ein Gerücht genügte, eine Bemerkung eines neidischen Nachbarn, eine Verdächtigung eines Bekannten – für die Stasi war jeder ein Feind. Und alles war ihr Recht, um mehr über die vielen Feinde zu erfahren, die sie überall sah.

In den Stasi-Akten standen Freunde und Kollegen als Zuträger, Männer, die ihre Frauen bespitzelten und Kinder, die ihre Eltern verrieten. Die Gründe dafür waren so banal wie niedrig: Geld, Eitelkeit, Missgunst. Jeder konnte zum Opfer werden, einfach so, ohne die Chance, es zu verhindern oder seine Unschuld zu beweisen.

Warum erzähle ich das alles? Der Gedanke, dass die allgegenwärtige Technik in unserem Leben dazu benutzt werden kann, uns auszuspähen, ist den meisten von uns schon lange gewärtig. Der Chaos Computer Club warnt seit vielen Jahren davor, dass Handys »Ortungswanzen« sind, die alles über ihren Besitzer verraten. Spätestens seit den Anschlägen vom 11. September werden immer mehr Gesetze verabschiedet, die

Bürgerrechte einschränken und die Macht des Staates ausdehnen, die Überwachung zulassen, auch auf einen vagen Verdacht hin.

Trotzdem ließ sich das Monster bis zum Juni 2013 noch gut verdrängen. Der so verführerische wie gefährliche Satz, dass wer nichts zu verbergen hat, auch nichts zu befürchten habe, wurde von allzu vielen allzu gern geglaubt. Diejenigen, die vor allwissenden Geheimdiensten und einem misstrauischen, allmächtigen Staat warnten, wurden als Alu-Hüte verspottet, als Verschwörungstheoretiker und Sonderlinge.

Edward Snowden hat das geändert. Edward Snowden hat uns dank seiner mutigen Tat unsere Akten zugänglich gemacht. Und sie sind – selbst für jene, die es schon länger ahnten – ein Schock.

Wir wissen noch gar nicht so viel darüber, wie genau die ganzen Spionageprogramme von NSA, GCHQ, BND und wie sie alle heißen funktionieren. Dazu sind die von Snowden veröffentlichten Unterlagen zu vage und zu überblicksartig. Es sind fast ausschließlich Powerpoint-Folien, in denen stichpunkthaft über diese Projekte informiert wird. Nirgends finden sich bislang technische Beschreibungen, Organigramme oder konkrete Zahlen.

Doch das, was wir dank Edward Snowden wissen, genügt, um eigentlich auch dem Letzten klar zu machen, dass die Regierungen der Welt die Technik des Internets und des Mobilfunks missbrauchen, um ihre Bürger – uns – nahezu vollständig zu überwachen. Es braucht nicht einmal mehr ein Gerücht oder einen Verdacht, jeder ist das Ziel dieser Ausspähung. Mit der Begründung, wer eine Nadel finden wolle, müsse eben den ganzen Heuhaufen durchsuchen, wird inzwischen alles gefiltert und gespeichert, was es an elektronischer Kommunikation gibt.

- Die Geheimdienste schneiden große Teil der Daten mit, die über die internationalen Seekabel laufen, nach Angaben der NSA sind das 29 Petabyte am Tag, 1,6 Prozent des gesamten Netztraffics[2], eine sicher geschönte Zahl.
- Die Geheimdienste kopieren Metadaten von Telekommunikationsverbindungen bei den Anbietern in unbekannter

Menge und aggregieren daraus Bewegungsprofile und Analysen der privaten Netzwerke der Abgehörten.

- Die Geheimdienste filtern und speichern E-Mails in unbekannter Menge und für eine unbekannte Zeit, wenn die E-Mails verschlüsselt sind wahrscheinlich für ewig.
- Die Geheimdienste überwachen via Internet geführte Gespräche mit Skype und anderen Messengerdiensten und speichern auch SMS in unbekanntem Umfang.
- Die Geheimdienste hacken die Computer von Telefonbetreibern, um die eigentlich verschlüsselt übertragenen Gespräche von Mobiltelefonen abhören zu können.
- Die Geheimdienste kopieren Daten von Finanztransaktionen, um Kontobewegungen verfolgen zu können.
- Die Geheimdienste beobachten Kommunikation in sozialen Netzwerken wie Facebook und sammeln die dort öffentlich zugänglichen Informationen aus den Accounts, um Profile von den Vorlieben und Vorstellungen der Überwachten zu erstellen und um zu erfahren, mit wem diejenigen Kontakt haben.
- Die Geheimdienste lesen Blogs und was sonst noch so in Newsgroups und Foren öffentlich im Netz verfügbar ist und werten diese Informationen aus.
- Die Geheimdienste geben Milliarden von Dollar aus, um Verschlüsselungsverfahren zu knacken oder zu unterwandern.

Mit anderen Worten: Unsere Geheimdienste tun alles dafür, dass wir keine Geheimnisse mehr haben, gar keine.

Und wer jetzt glaubt, dass davon ja nur andere betroffen sind und nicht er selbst – immerhin dürfen Geheimdienste wie NSA, GCHQ oder BND laut den Gesetzen ihrer Länder nur Ausländer überwachen und nicht die eigenen Bürger –, der darf nicht vergessen, dass eben diese Geheimdienste ihre Erkenntnisse gern und oft miteinander tauschen. Was der eine offiziell nicht erfahren darf, das darf der andere ganz problemlos. Denn, wie der Spontispruch sagt, jeder ist Ausländer, fast überall.

Und wer jetzt glaubt, dass davon ja nur Terroristen betroffen sind und andere Bösewichter, der darf nicht vergessen, dass bereits ein Gerücht, eine böse Bemerkung, eine Verdächtigung oder auch ein Zufall genügen, um diesen riesigen Spähapparat auf Touren zu bringen. Und dass die Betroffenen keine Chance haben, ihre Unschuld zu beteuern, weil sie im Zweifel gar nicht erfahren, dass sie minutiös überwacht werden und weil jede Bewegung, jede Handlung ihnen zum Schlechten ausgelegt wird und ganz bestimmt nicht zum Guten und zu ihrer Entlastung.

Die Stasi ließ sich ignorieren, zumindest bis ihre Akten zugänglich wurden. Die Bedrohung durch den technischen Überwachungsstaat ließ sich ignorieren, bis Edward Snowden uns die Akten der Überwacher zugänglich gemacht hat.

Die Stasi hat sich erledigt, weil viele Tausende mutige Menschen monatelang auf die Straße gingen und letztlich den Staat zu Fall brachten, der das Ministerium für Staatssicherheit geschaffen hatte. Zu glauben, dass nun überall auf der Welt Menschen demonstrieren und die Regierungen der halben Welt stürzen, ist eine Illusion. Aber zu glauben, dass überall auf der Welt mutige Menschen auf die Straße gehen und mehr Bürgerrechte fordern, mehr staatliche Transparenz, engere Grenzen für Geheimdienste und besseren Schutz vor ihnen, ist keine Utopie. Immerhin leben wir in Demokratien, wir wählen diejenigen, die die Gesetze machen.

Offensichtlich ist nur noch nicht genug Menschen aufgegangen, wie wichtig es ist, dass keine solchen Monster unter uns leben. Denn das Problem ist das Misstrauen, das sie säen. Früher richtete es sich gegen den Nachbarn und die Freunde, letztlich gegen jeden, denn jeder konnte einen verraten. Es zerfraß die Gesellschaft. Das Monster ließ sich zwar verdrängen, glücklich aber wurde damit niemand, die Angst blieb. Bei jedem Witz, den man erzählte, bei jeder Kritik, die man äußerte, war die Angst mit dabei. Heute richtet sich das Misstrauen gegen die Technik. Jedes Gespräch, jede Verbindung, jeder Datenaustausch kann uns verraten und uns zu Verdächtigen machen. Das Internet, das so viel Positives ermöglicht, wird von den Geheimdiensten als Waffe gegen uns missbraucht.

Es macht keinen Unterschied, ob wir unseren Gegenüber fürchten oder das Gerät in unserer Hosentasche. Beides sind unsere Netzwerke, die uns bestimmen, in denen wir hängen und ohne die wir nicht leben können.

Das 2008 formulierte IT-Grundrecht, das eigentlich Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme heißt, beschreibt, worum es geht. Im Urteil des Bundesverfassungsgerichtes, das dieses Grundrecht schuf, heißt es: »Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit. Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist. [...] Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. [...] Viele Selbstschutzmöglichkeiten – etwa die Verschlüsselung oder die Verschleierung sensibler Daten – werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in

Zukunft verbleiben, sich technisch selbst zu schützen. Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet.«

Doch der Staat achtet die Vertraulichkeit der Technik nicht. Es wird Zeit, dass wir etwas dagegen tun, bevor die Zahl der Opfer der Überwachung so groß ist, dass wir sie nicht mehr ignorieren können. Wir sollten uns dagegen wehren, technisch und politisch.

Verschlüsselung ist Bürgerpflicht, sagt Phil Zimmermann, der das Programm *Pretty Good Privacy* entwickelt hat. Wer seine Daten verschlüsselt, schützt nicht nur sich selbst, sondern auch viele andere, die das noch nicht können und noch nicht tun. Wer seine Kommunikation verschlüsselt, sorgt mit dafür, dass es zur Normalität wird, zum Standard. Auch wenn das keine Überwachung verhindert, macht Verschlüsselung es doch den Überwachern schwerer.

Und es wird Zeit, dass wir für unsere Rechte auf die Straße gehen und dafür demonstrieren, nicht mehr überall und jederzeit überwacht zu werden. Im Zweifel jeden Montag.

Die Welt nach PRISM: Lektionen und ein überfälliger Anfang

Georg C. F. Greve

Die Utopie des frühen Internet war die Behauptung, es fördere qua seiner naturgegebenen Eigenschaften die Demokratie und führe zu einer Gesellschaft, in der Regierungen zum Auslaufmodell gehören. Auch wenn die Mauer um diese Utopie schon eine ganze Weile bröckelte: PRISM hat sie endgültig niedergerissen. Bruce Schneier nennt das Internet daher vielmehr einen Macht-Multiplikator: Wer bereits viel Macht hatte, wird gestärkt. Wer weniger Macht hatte, gewinnt auch dazu, aber der Abstand wächst. Viel spricht dafür, dass Schneier mit seiner Einschätzung Recht hat. Auch und gerade bei der stark wachsenden »Cloud«, für die anwendbares Recht weit vor Kryptografie oder technischer Sicherheit über die wahre Kontrolle der Daten entscheidet.

Der Grund für diese Eigenheiten wird offenbar, wenn man sich die Konsequenzen des selben latenten Anarchismus vor Augen führt, der auch die Argumente für die inhärente Demokratieförderung liefert. Wo jeder Akteur direkt auf Basis seiner individuellen Fähigkeiten mit jedem anderen Akteur interagiert, steht der einzelne Bürger der Staatsmacht eines jeden Landes direkt gegenüber. Die größte Konzentration von nicht-staatlicher Macht befindet sich in den großen Internet-Unternehmen. Diese sind jedoch weit weniger extraterritorial als sie uns glauben machen wollen. Vielmehr nehmen sie eine De-fakto-Ausweitung des US-Rechts auf die ganze Welt vor, gestützt durch Abkommen wie Safe Harbor. Das Europäische Datenschutzrecht ist hier weitestgehend entkräftet und der Schutz, den die US-Unternehmen versprechen, wird meist nur aufgrund der nahezu bedingungslosen Offenlegung intimer Details und der Erlaubnis, diese kommerziell zu verwerten, gewährt. Der Vergleich mit Feudalherren ist daher nicht völlig abwegig, um die Beziehung zu beschreiben. Nun ist die Rückkehr

ins Feudalsystem allerdings eher das Gegenteil der versprochenen Demokratisierung, unter der diese Dienste beworben wurden.

Daher gehören die Vertreter der Utopie oft auch zu den schärfsten Kritikern der Internetlords. Die oft gepredigte Antwort auf die Feudalherren ist Dezentralisierung, Föderalisierung, Selbsthosting. Es sollen also alle Menschen ihre Technologien mit Freier Software auf eigenen Servern selbst betreiben. Nur gibt es gute Gründe, diese Antwort zumindest in ihrer Absolutheit als zynisch zu betrachten. Vielen Menschen fehlen nicht nur die finanziellen Mittel, um einen eigenen Server zu unterhalten, der großen Vielzahl an Menschen fehlt vielmehr die Kompetenz, ja sogar der Wunsch nach dieser Kompetenz. Und das wird sich trotz aller Versuche der Umerziehung auch nicht ändern. Denn für den Großteil der Menschen ist die Technologie schlicht ein Werkzeug für einen bestimmten Zweck, nicht aber Selbstzweck. Ohne dies untermauern zu können, würde ich sogar vermuten, dass eine überraschend große Zahl der Nutzer dieses Werkzeug lieber aufgeben würde, wenn die einzig verbleibende Alternative der entsprechende Aufbau von Kompetenz wäre.

Eine häufige Reaktion auf dieses Problem ist die Bereitstellung von vereinfachten, bereits vorkonfigurierten Lösungen. Nur ist die Zielgruppe für derartige Lösungen letztlich dieselbe Gruppe, die auch sonst selber eigene Infrastruktur betreiben könnte. Denn die Komplexität der Lösungen ist ein Resultat der Vielfalt der Möglichkeiten und Anwendungsfälle und nicht einer Verschwörung mit dem Ziel, die Nutzung dieser Technologien zu erschweren. Komplexität zu reduzieren, dabei nicht zu viele Annahmen und Einschränkungen zu machen, die Sicherheit nicht zu kompromittieren, all dies sind extrem schwere Aufgaben. Nahezu alle Techniker unterschätzen diesen Teil systematisch. Daher ist es auch kein Zufall, dass bisher nur in den seltensten Ausnahmen eine derartige Kombination gelang – und meines Wissens niemals ohne erhebliche Investition in die nicht-technischen Bereiche.

Das Ergebnis ist also auch hier wieder letztlich eine Form der libertären Gesellschaft, in der Einzelne dem Offensivpotential der NSA oder

vergleichbarer Organisationen anderer Länder im Wesentlichen ausgeliefert sind. Zumal dieser Macht nahezu keine rechtlichen Rahmenbedingungen gesetzt sind. Geheimdienstliche Tätigkeit läuft außerhalb des sonstigen rechtlichen Rahmens. Das ist auch in Deutschland so, wo Artikel 10 des Grundgesetzes eine entsprechende Ausnahme vorsieht. Und da die Geheimdienste eng vernetzt sind, werden bestimmte Tätigkeiten dort vorgenommen, wo dies möglich ist und dann im Rahmen von geheimdienstlicher Kooperation mit anderen Diensten ausgetauscht. Dabei dienen gesammelte Daten als »Pseudowährung«, mit der Zugang zu anderen Quellen oder Erkenntnissen erkauft wird.

Aber vermutlich wird schon die reine Ökonomie diesen Schritt verhindern. Denn ohne Frage ist die Skalierung der Kosten im Rechenzentrum um Größenordnungen besser. Und auch die Frage der Betriebssicherheit ist nicht von der Hand zu weisen. Ein System ohne regelmäßige Wartung durch einen Administrator ist verwundbar. Spätestens bei der Vorstellung von hunderten von Millionen von Systemen ohne Administrator verteilt über die ganze Welt sollte man hellhörig werden. Es gibt also ein starkes Argument gegen Selbsthosting auf Seiten der Wirtschaft und der Sicherheit.

Es gibt durchaus Versuche, diese Lücke zu schließen, sei es auf Ebene teilweise eher anarchisch gefärbter Kollektive, oder auch über Unternehmen, welche sich in diesem Bereich positionieren. Allerdings führt hier die richtige Motivation oft zu Ansätzen, welche sich als »Digitales Dumpster Diving« charakterisieren ließen. Das Dumpster Diving kann nur auf Basis einer Konsumgesellschaft existieren. Es produziert selber nichts. Ganz ähnlich werden hier von manchen Anbietern Technologien eingesetzt, zu denen nichts beigetragen wird. Das kannibalisiert damit potentiell diejenigen, die derartige Technologien entwickeln, bzw. übt Druck auf sie aus, die Technologie zu proprietarisieren. Die Nachhaltigkeit derartiger Ansätze beruht also ausschließlich auf der anhaltenden Offenheit Dritter.

Leider gibt es hier nur wenige Ausnahmen und diese Fragen sind noch nicht ins Bewusstsein der Nutzer gelangt. Sie spielen daher keine Rolle

in deren Kaufentscheidung. Das gilt auch für die globale Ausweitung des US-Rechts auf Nutzer weltweit durch Nutzung entsprechender Dienste. Und schließlich fokussiert sich die Debatte aktuell zu sehr auf die Internet-Giganten und die NSA, wodurch vielen anderen Fragen keine Aufmerksamkeit mehr zukommt. Die Nutzung der Geheimdienste, insbesondere zur Erlangung wirtschaftlicher und politischer Vorteile, ist in vielen Ländern verbreitet und nicht erst seit Edward Snowden die PRISM-Dokumente geleakt hat.

Seit es das Internet gibt haben sich aber die Möglichkeiten dramatisch entwickelt, während die Politik sich mit der Regulierung eher schwer tat. Dies lag auch an den Vereinigten Staaten von Amerika selbst, welche kurioserweise teilweise mit Unterstützung der Netzgemeinde Versuche zur Regulierung erfolgreich abgewehrt haben. Die utopische Vision vor Augen wurde einer Nichteinmischung durch Regierungen der Vorzug gegeben. Mehr als einmal haben wir damals das Argument gehört, dass, wenn alle Länder erst einmal voll ans Internet angebunden wären, die Demokratie quasi automatisch folgen würde. Das muss man aus heutiger Sicht als Fehleinschätzung bewerten.

Die Freie-Software-Gemeinschaft war schon damals zumindest insofern weiter als sie verstanden hatte, dass sich durch Software eine Machtfrage stellt. Die Konzentration dieser Macht in den Händen Einzelner ist ein gesellschaftliches Problem. Ein Zusammenhang, der u.a. durch die erwiesene Zusammenarbeit von proprietären Softwareunternehmen mit der NSA aufs Dramatischste bestätigt wurde. Der ehemalige Microsoftmitarbeiter Caspar Bowden erklärte im Europäischen Parlament, dass er der Software von Microsoft nicht mehr traut und nunmehr auf Freie Software setzt und empfiehlt sie für den Regierungseinsatz. Freie Software spielt in allen Szenarien für die Sicherung der Privatsphäre eine entscheidende Rolle. Nur sagt beispielsweise Bruce Schneier auch, dass seine Tipps für die Wahrung der Sicherheit Mist sind, weil ein Großteil der Bevölkerung sie nicht umsetzen kann.

Die Frage, wie Softwarefreiheit allgemein nutzbar wird, ist durch PRISM auch für Außenstehende als ein entscheidender Meilenstein für eine

freiheitliche und demokratische Gesellschaft sichtbar geworden. Dies wird uns aber nur gelingen, wenn Überwachung nicht länger das allgemein akzeptierte Geschäftsmodell des Internets darstellt. Leider ist die Welt der Überwachung attraktiv und bequem. Der Nutzen ist für jeden Anwender täglich erfahrbar. Der Preis ist es nicht. An diesem Problem arbeiten sich Befürworter von Freier Software in unterschiedlichen Ausprägungen seit den 80er Jahren ab. Anbei ein paar Anregungen für Komponenten einer notwendigerweise komplexen Antwort auf dieses komplexe Problem.

Die individuellen Kosten mögen schwer zu erfassen sein. Die politschen und wirtschaftlichen Kosten von Spionage und Manipulation sind es nicht. Die brasilianische Präsidentin Dilma Rousseff sagte in ihrer Rede vor der Hauptversammlung der Vereinten Nationen, dass die Souveränität eines Landes dort aufhört, wo sie die Souveränität eines anderen Landes beschneidet. Das klingt nicht nur zufällig so ähnlich wie die in der GNU GPL kodifizierte Freiheit und deren Bewahrung durch das Copyleft, es ist ein fundamentales humanitäres Prinzip für eine freiheitliche Gesellschaft.

Es geht also darum, den politischen Dialog um souveräne Software auf allen Ebenen fortzuführen. Dabei ist es durchaus gesund, nationale Interessen im Blick zu halten, denn auch die politische Legitimation entsteht auf Ebene von Nationalstaaten. Kurzfristige Maßnahmen können durch entsprechende Strategien für Freie Software und Offene Standards im Regierungseinsatz ergriffen werden. Dies sollte flankiert werden mit entsprechenden Informationen für die Wirtschaft, um dem einzelnen Unternehmen den nachhaltigen Schutz vor Wirtschaftsspionage zu ermöglichen. Mittelfristig braucht es belastbare internationale Vereinbarungen zum Umgang mit modernen Technologien.

Gerade im Sicherheitsbereich ähnelt die Situation in mancher Hinsicht dem Klischee vom wilden Westen, wo gerne auch mal die Schurken zum Sheriff ernannt wurden und die Zivilisten dieser Elite nicht viel entgegenzusetzen hatten. Axel Arnbak von Bits of Freedom spricht in diesem Zusammenhang von der »dubiosen Rolle der Akademiker«,

welche Technologien in die Welt setzen und verbreiten, teilweise mit, teilweise ohne Bezahlung, auf welche die Breite Masse der Bevölkerung nicht vorbereitet ist und gegen die es keine realistischen Schutzmaßnahmen gibt. Zu diesen Akademikern gehören dabei nicht nur traditionell in der Universität beheimatete Wissenschaftler, sondern letztlich alle, die neue Wege beschreiten. Gesellschaftlich besteht die große Herausforderung also darin, den Vorsprung durch das Herrschaftswissen der technischen Elite einer gesellschaftlichen Aufsicht zu unterstellen. Es geht darum, die Macht der Elite, zu der wir letztlich alle gehören, gewissen Schranken und Regeln zu unterwerfen. Diesen Dialog sollten wir jetzt aktiv führen, um sinnvoll am Dialog auf politischer Ebene mitwirken zu können, sonst wird er uns irgendwann aufgezwungen.

Wo diese Debatte bereits stattfindet, ist teilweise auf Ebene der Infrastruktur und zum Teil auf Ebene der Inhalte. Im Normalfall ist der Tenor dort Deregulierung, da die Internet-Giganten über durch sie finanzierte Think-Tanks mit ensprechenden Stellen ihr finanzielles Kapital in politischen Einfluss ummünzen. Dies wird möglich durch manche Aktivisten, die sich teils mit Blick auf die »Yuppie Nuremberg Defense« vereinnahmen lassen. Die Unabhängigkeit der Wissenschaft gilt es jedoch auch in diesem Bereich wiederherzustellen und zu bewahren, der Rest sollte über ein Lobbyregister transparent gemacht werden. Denn natürlich ist es legitim, eigene Interessen zu vertreten. Es sollte nur klar sein, wessen Interessen vertreten werden. Daher wird die Bedeutung von Organisationen wie der FSFE oder digitalcourage in Zukunft eher zunehmen und sie sind der richtige Ort um sich zu engagieren, wenn man an den gesellschaftlichen Fragen Interesse hat.

Ein derartiger Dialog muss aber immer nach vorne gerichtet sein. So ist die Aufforderung einer Abkehr vom »Cloud Computing« aus meiner Sicht unrealistisch und zeigt ein Unverständnis von modernen Technologien, Nutzungsmustern, und ökonomischer wie ökologischer Effizienz. Es gibt zudem keine realistische Alternative. Wir müssen also Prinzipien entwickeln, nach denen derartige Dienste operieren, wie wir es beispielsweise bei MyKolab.com versucht haben, mit klarem Bekenntnis zur Entwicklung aller Technologien als Freie Software,

starkem Datenschutz und verlässlicher Privatsphäre, geschützt durch die lokale Gesetzgebung. Ob dies ein Weg für die Zukunft sein kann, wird sich über die Nutzung entscheiden. Es läuft also auf die bewusste Kaufentscheidung hinaus. Dafür braucht es aber Klarheit darüber, was die Nutzungsbedingungen wirklich sagen. Aus diesem Grund ist das »Terms of Service; Didn't Read«-Projekt so wichtig, denn es macht das Geschäftsmodell Überwachung transparent und erlaubt den Vergleich zwischen Anbietern.

Die Werte der Aufklärung bildeten eine zentrale Grundlage für die Einführung der Demokratie. Es ist Zeit, sie auch auf die digitale Welt anzuwenden, denn die Lektion von PRISM ist recht eindeutig. Auch wenn Europa eine nie dagewesene Periode des zivilisierten Friedens erlebt hat und eine ganze Generation das Glück hatte, davon geprägt zu werden: In den USA und den meisten anderen Ländern der Welt wurde die Macht- und Realpolitik niemals beendet, sie wurde nur besser verborgen. Insbesondere die Wirtschaftspolitik mittels Spion wird nicht über Nacht verschwinden und daher noch eine Weile Bestand haben. Auch darauf müssen wir uns einstellen. Sie wird sich nur beenden lassen, wenn eine gemeinsame Grundlage besteht und wir es schaffen, zunehmend zu einem globalen Wertekanon zu kommen, der die digitale Welt nicht länger ausklammert.

Dies sind also die Fragen, die sich in vielfältiger Ausprägung sowohl national wie international stellen. Es würde dabei nicht überraschen, wenn in etlichen Jahren rückblickend PRISM als der Moment wahrgenommen würde, an dem die Informationstechnologie ihre Pubertät abschloss und es Zeit wurde, erwachsen zu werden. Ein solcher Prozess wird sicher anstrengend und teilweise auch sehr kontrovers werden. Gleichzeitig darf man sich durchaus darauf freuen. Es geht um nicht weniger als die Zukunft der Gesellschaft mit so zentralen Fragen wie der Wahrung der Privatsphäre, ohne die es keine freie Meinungsäußerung und auch keine echte Demokratie geben kann. Wir sind an einem Punkt, wo wir diese Debatte und damit auch die zukünftige Gesellschaft entscheidend mitgestalten können.

Eine große Aufgabe also, an der wir als globale Gesellschaft gemeinsam wachsen dürfen.

Was will man mehr?

Snowden und die Zukunft unserer Kommunikationsarchitektur

Jérémie Zimmermann

Snowdens Enthüllungen werfen ein Licht auf Sachverhalte, die uns dazu zwingen, uns wichtige Fragen zu stellen und Maßnahmen zu ergreifen, die essentiell für die Zukunft unserer Online-Gesellschaften und sogar die Struktur unserer politischen Systeme werden könnten.

Die geleakten Dokumente belegen, was viele Hacker und Bürger schon geahnt haben: Eine umfassende Pauschal-Überwachung der persönlichen Kommunikation im Internet durch die NSA. Was vor einigen Monaten oft noch als Verschwörungstheorie oder Verfolgungswahn abgetan wurde, war tatsächlich nah an der kruden Realität.

Die wichtigste Tatsache, die wir aus Snowdens Enthüllungen erfahren haben, ist das gewaltige Ausmaß der Überwachung: Die Anzahl von 97 Milliarden Datensätzen (Informationsteilchen), die alleine im Monat März 2013 gesammelt wurden (alleine durch PRISM - das nur *eines* der Programme der NSA ist!) gibt einen Einblick, wie umfassend die Bespitzelung der Bürger der Welt ist. Die armselige Verteidigung der US-Regierung, die Aussage »keine Sorge, nur Nicht-US-Bürger sind das Ziel«, sollte ins Verhältnis gesetzt werden zu der Tatsache, dass die Zielauswahl bestimmt wird durch eine Bewertung mit einer »mindestens 51-prozentigen Chance, dass jemand Nichtausländer ist« - im Prinzip also das Werfen einer Münze plus 1% ... Falls du zufällig jemanden kennst, der zufällig jemanden kennt, der möglicherweise etwas tun könnte, was als falsch angesehen wird, dann ist es wahrscheinlich, dass deine gesamte persönliche Kommunikation abgehört wird. Falls du Journalist bist und versuchst, deine Quellen zu schützen, ein Rechtsanwalt oder ein Arzt, der ein Arztgeheimnis schützt, ein Politiker usw., dann bist du dabei.

Die andere bedeutende Tatsache ist die aktive Mitarbeit von Google, Facebook, Apple, Microsoft und ähnlichen riesigen Internet-Konzernen: Ob sie durch Geheimgesetze und ein Geheimgericht zur Mitarbeit gezwungen wurden oder ob sie freiwillig kooperieren tut nicht viel zur Sache. Bedeutsamer ist, dass es nun offensichtlich ist, dass diese Unternehmen nur Erweiterungen der völlig außer Kontrolle geratenen US-Geheimdienste sind - abgedriftet in eine paranoide Richtung, welche die Rechte von Bürgern in der ganzen Welt gefährdet. Durch die Nutzung ihrer Dienstleistungen und Produkte ist jeder der Gefahr ausgesetzt, transparent zu werden, abgehört, beobachtet, jeder Tastenanschlag potenziell aufgezeichnet. Die Enthüllungen über PRISM sagen uns, dass man diesen Unternehmen, ihren Produkten und Dienstleistungen nicht trauen kann. Sie veranschaulichen, was Befürworter von freier Software und andere Verteidiger der Freiheit im Internet schon seit langem sagen: Die sehr technische und ökonomische Prägung dieser zentralen Dienste verwandelt sie in gigantische Spionage-Maschinen. Das Wesen dieser proprietären Systeme und der nicht quelloffenen Software verwandelt sie in Instrumente der Kontrolle.

Ebenfalls von grundlegender Bedeutung ist das Sabotieren von jeglichen kommerziellen Sicherheitsprodukten, die Verschlüsselungstechnologie bieten. Pro Jahr wurden 250 Millionen Dollar in das Programm »Bullrun« investiert, um kommerzielle Kryptographie zu schwächen, wodurch quasi offene Löcher in der weltweiten Sicherheits-Infrastruktur hinterlassen wurden, egal ob es um das Abrufen Ihrer E-Mails, die Kommunikation mit einer Verwaltung oder einem Unternehmen, um Shopping oder Online-Banking geht.

Schließlich haben wir erfahren, dass die NSA die Kommunikation von Petrobras, dem wichtigsten brasilianischen Energieunternehmen, und die persönliche Kommunikation von Dilma Rousseff, der brasilianischen Präsidentin, ausspioniert hat. Jeder Versuch, die Massenüberwachung mit ihrer Effizienz und Verhältnismäßigkeit im Kampf gegen den Terrorismus zu rechtfertigen, ist damit obsolet: Da weder das Unternehmen, noch das Staatsoberhaupt ernsthaft als des Terrors verdächtig betrachtet werden können, ist es nun offensichtlich, dass

diese massive globalisierte Überwachung auch für wirtschaftliche Informationen und politische Überwachung eingesetzt wird, um die Interessen der USA und ihrer Unternehmen zu bedienen.

All diese Einzelheiten zusammengenommen verraten uns eine Menge über den gegenwärtigen Stand der Technologie und die Verbindung zwischen Technologiekonzernen und der US-Regierung. Wir sollten uns nun fragen, wie wir die Kontrolle über unsere persönliche Kommunikation und unsere Daten zurück erlangen, wie wir uns dieser ungerechtfertigten massiven Überwachung entziehen und unsere digitale Souveränität zurückgewinnen können.

Mit Sicherheit wird es einige Zeit brauchen, um eine Alternative zu dieser orwellschen Überwachung zu erschaffen. Aber es ist eine Anstrengung, die im Interesse zukünftiger Gesellschaften, in denen unser Grundrecht auf Privatsphäre eine Bedeutung hat, unternommen werden muss. Tatsächlich ist es eine Aufgabe von politischem und gesetzgebendem Charakter, aber ebenso auch eine technologische und (wenn nicht sogar hauptsächlich) soziale Aufgabe.

Auf rein politischer Seite ist es offensichtlich, dass die Gesetze der USA geändert werden müssen und dass die US-Bürger Kontrolle über die NSA bekommen müssen. Dass ganze Teile der öffentlichen Politik, ein spezielles Gericht, seine Entscheidungen und spezielle Interpretationen des Gesetzes vor der Öffentlichkeit geheim gehalten werden, ist nicht vereinbar mit einer demokratischen Gesellschaft, die am Prinzip der Rechtsstaatlichkeit und der Gewaltenteilung festhält. Für uns, die wir nur Bürger von »more than 51% foreignness« (»über 51% Fremdheit«) für die USA sind, könnte das ein Ziel außerhalb der Reichweite sein … alles, was wir tun können, ist, den politischen Druck auf die US-Regierung zu erhöhen und US-Aktivisten zu unterstützen, darauf zuzuarbeiten.

Hier in der EU erfordern die Enthüllungen von Snowden eine starke politische Reaktion der Entscheidungsträger, die bisher sehr zahm waren … Zum Beispiel da jede einzelne Verpflichtung aus dem »Safe Harbor«-Abkommen, das US-Unternehmen von der Beachtung der EU-Rechtsvorschriften über den Schutz personenbezogener Daten

entbindet, ganz offensichtlich gebrochen wurde. Nun ist die EU formal in der Lage, es zu widerrufen. Dies würde es ermöglichen, mit Oberhand für die EU eine neue Vereinbarung auszuhandeln, während US-Konzerne, die für die Überwachung verantwortlich sind, hart abgestraft werden (was sich für Unternehmen in der EU wiederum positiv auswirken könnte). Ein solch mutiger politischer Schritt scheint bisher nirgendwo in Aussicht zu sein.

Wir müssen auch politische Entscheidungsträger dazu drängen, einen starken, wirksamen Schutz unserer persönlichen Daten gesetzlich zu verfügen. Die Datenschutzverordnung, über die derzeit im EU-Parlament debattiert wird, steht in Begriff, ihrer Substanz beraubt zu werden - unter dem mächtigen Einfluss von genau jenen Firmen, die auf frischer Tat dabei ertappt wurden, wie sie sich an der massiven Überwachung beteiligt hatten. Die Bürger müssen sich in diese öffentliche Debatte einmischen, um sicherzustellen, dass starke Hindernisse gegen den Export ihrer Daten in ausländische Zuständigkeitsbereiche (Gerichtsbarkeiten) errichtet werden und dass ihnen wirksame Werkzeuge gegeben werden, um Kontrolle über ihre persönlichen Daten und Kommunikation wiederzuerlangen.

Auf der anderen Seite müssen EU-Bürger von ihren Politikern neuen Rechtsschutz für Whistleblower und für die Freiheit der Meinungsäußerung und Kommunikation im Allgemeinen verlangen, denn die Verfolgung von Manning, Assange und jetzt Snowden zeigt, dass sie unter ungeheuer unverhältnismäßigen Kosten für ihr eigenes Leben aktiv wurden, obwohl sie damit doch offensichtlich dem Allgemeininteresse dienten.

Schließlich müssen wir unsere politischen Entscheidungsträger dazu drängen, in der EU und in den verschiedenen Mitgliedsstaaten gesetzlich eine starke Industriepolitik zu etablieren, welche Technologien anregt, fördert und finanziert, die das Individuum eher befreien, anstatt es zu kontrollieren und auszuspionieren.

Dieser technologische Aspekt ist der Schlüssel. Wir haben jetzt eine klare Sicht auf die Entwurfsmuster für Technologien, die Individuen kontrollieren: zentrale Dienste (basierend auf der Anhäufung möglichst

vieler Daten), geschlossene proprietäre Software und Systeme sowie unzuverlässige Verschlüsselung, bei der Vertrauen in die Hände von Dritten übergeben wird.

All diese Muster führen zu Technologien, die uns unserer persönlichen Daten enteignen, und unsere Kommunikation der Gnade der NSA, ihrer Verbündeten und ihrer hundert privaten Vertragspartner überlassen.

Auf der anderen Seite geben uns die Enthüllungen Snowdens ein anschauliches Beispiel, dass Richard Stallman und andere all die Jahre Recht hatten. Tatsächlich haben wir die Entwurfsmuster für Technologien, die Personen eher befreien können anstatt sie zu kontrollieren, bereits auf dem Tisch liegen:

- Dezentrale Dienstleistungen: Idealerweise Daten selbst hosten oder allenfalls von einer überschaubaren Menge an Menschen, wie einer Handvoll Freunde, einem Unternehmen, einer Universität, einem Verein, etc. Dies ist der Preis dafür, dass wir uns nicht daran beteiligen, (Daten-)Anhäufungen zu bilden, die diese Unternehmen enorm leistungsstark und zu einem strukturellen Teil des Überwachungsstaats machen.

- Freie Software: Allen Nutzern dieselben Freiheiten zu geben, die der ursprüngliche Urheber der Software hatte, ist der einzige Weg für Menschen, eine Möglichkeit zur Kontrolle ihres Gerätes zu haben, statt andersherum. Freie Software macht den Austausch von Wissen und Fähigkeiten zu digitalem Gemeingut. Wie »Bullrun« zeigt, kann man Kryptografie und anderen Sicherheits-Tools, die nicht nach den Grundsätzen freier Software aufgebaut sind, niemals trauen. Punkt. (Die Frage danach, wie man Zugang zu den Spezifikationen der Hardware bekommen kann, auf der wir diese Software betreiben, muss in der Tat gestellt werden, da die zunehmende Verwendung von black-boxed Hardware es einfach macht, Backdoors einzubauen, die gegen uns verwendet werden können. Regierungsbehörden könnten Hersteller dazu zwingen, die wichtigsten Spezifikationen offen zu legen. Vielleicht können wir eines Tages offene Hardware bauen, der wir vertrauen können ...)

- Ende-zu-Ende-Verschlüsselung, bei der die Mathematik garantiert, dass nur der Benutzer und die Menschen, mit denen sie oder er kommuniziert, die Möglichkeit haben, die Inhalte ihrer Kommunikation abzurufen und zu lesen, unter Ausschluss von Dritten wie Google, Facebook, Skype, Apple, usw. Das bedeutet, dass die Nutzer dahin kommen müssen, die grundlegenden Konzepte zu verstehen und in der Lage sein müssen, ihre Schlüssel zu verwalten, was nicht so selbstverständlich ist, wie es klingt, wie wir in den letzten Jahrzehnten gesehen haben ...

Letzten Endes können die politischen und technologischen Dimensionen vom Aufbau einer Welt, in der die Technologie Nutzer und Gesellschaften freier macht, anstatt sie zu kontrollieren und auszuspähen, in der Praxis möglicherweise nur durch eine dritte, soziale Dimension artikuliert werden.

Dieses Ziel können wir wahrscheinlich nur erreichen, wenn wir es schaffen eine Dynamik zu erzeugen, um unsere Kollegen, Freunde und die Gesellschaft als Ganzes dahin zu führen, dass sie begreifen, warum es von entscheidender Bedeutung ist, die zentralisierten, geschlossenen Services und Produkte hinter sich zu lassen und zu Technologien zu wechseln, die befreien; nur wenn es uns gelingt, genügend Druck auf politische Entscheidungsträger auszuüben, nur wenn wir, als Individuen und als Gemeinschaften, anfangen, uns um die zugrunde liegenden baulichen Prinzipien unserer Kommunikationsinfrastruktur und -technologien zu kümmern. Es mag vielleicht schwierig klingen, aber nicht unerreichbar, denn dies ist wohl eines der wichtigsten Unternehmen für die Zukunft unserer Gesellschaften online, und wir alle spielen dabei eine Rolle.

Dieser Text wurde von der Redaktion ins Deutsche übersetzt.

Der Ausspähskandal – Weckruf für die Demokratie

Annette Mühlberg

Die Nachricht schlug hohe Wellen: Die National Security Agency (NSA) sammle von großen US-Providern Verkehrs- und Inhaltsdaten der Kunden ein und durchsuche diese gigantische Informationshalde mit modernsten Methoden nach möglichen Kennungen Verdächtiger, enthüllte der Whistleblower Edward Snowden im Juni 2013. Selbst Inhaltsdaten von E-Mails, Chats, Internet-Telefonaten oder Webdiensten großer US-Konzerne wie Facebook, Google, Microsoft oder Yahoo könnten abgerufen werden, erläuterte der frühere Zuarbeiter des technischen US-Geheimdienstes.

Seither veröffentlichen renommierte Medien schier wöchentlich weitere Bausteine der umfassenden Bespitzelung von Bürgern, Unternehmen & Politikern. Auch Banken und Kreditkartentransaktionen werden demnach von dem technischen US-Geheimdienst überwacht, ganze Provider und Knotenpunkte im Netz ausgespäht, soziale Beziehungen über Social Networks bis ins Detail rekonstruiert. Auch das europäische SWIFT-Netzwerk, das den internationalen Überweisungsverkehr abwickelt, wird umfangreich angezapft und der Zahlungsverkehr bei der NSA gespeichert. Horrorvisionen einer Big-Brother-Überwachung sind nicht mehr von der Hand zu weisen – mit massiven Auswirkungen auf Wirtschaft, Arbeitswelt und Gesellschaft.

In Deutschland hat sich das Bundesverfassungsgericht kontinuierlich mit der Frage des Verhältnisses von Datensammlungen und Demokratie auseinandergesetzt und dazu grundlegende Urteile gefällt, etwa zur Volkszählung 1983 und 2008 zur heimlichen Online-Durchsuchung mit der Definition des »Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme«. 2010 erzielten die Verfassungsbeschwerden gegen die Vorratsdatenspeicherung, die sowohl von tausenden Einzelpersonen als auch – insbesondere unter dem Gesichtspunkt Meinungs-, Presse- und Koalitionsfreiheit – von der Gewerkschaft ver.di eingelegt wurden, einen weitgehenden Erfolg. Auch

das Verfahren für den elektronischen Entgeltnachweis (ELENA) wurde im Folgejahr unter anderem aus Datenschutzgründen eingestellt. Unterdessen jedoch entstand eine geheimdienstliche Parallelwelt unter Freunden, die eben jene klar definierten Grundrechte hintergeht.

Frühere Agenten der NSA, die in den vergangenen Jahren öffentlich die Alarmglocken wegen Missständen in ihren Institutionen läuteten, sprechen angesichts der Enthüllungen ihres »Nachfolgers« Snowden vom Aufbau eines geheimen Überwachungsstaats im Namen einer falsch verstandenen nationalen Sicherheit. In den USA habe sich eine »weiche Tyrannei« herausgebildet, die Grundrechte mit Füßen trete, erklärte der NSA-Whistleblower Thomas Drake Ende September 2013 bei einer Anhörung im EU-Parlament. Diese Herrschaftsform sei besonders gefährlich, da sie »im Schatten des Rechtsstaats« ausgeübt werde.

Die NSA verletze Bürgerrechte im »industriellen Ausmaß«, führte Drake aus. Er sei beim Start der entsprechenden Programme dabei gewesen mit denen unter Verweis auf hochgespielte Gefahren möglichst viele »unserer Kommunikationsdaten« gespeichert und systematisch ausgewertet würden: »Jedes Detail unseres persönlichen Lebens wird zum Eigentum der Verwaltung erklärt und jahrelang in geheimen Dossiers aufbewahrt.« Parallel werde die Sicherheit im Internet massiv unterwandert. Die NSA nutze das »Drehbuch der Stasi« bewusst, so der Hinweisgeber, um die eigene Bevölkerung und die von Drittstaaten auszuspähen[3].

Dies gefährdet die Demokratie in mehrfacher Weise. Zum einen wird die Meinungs-, Presse- und Koalitionsfreiheit durch die anlasslose Überwachung unserer Kommunikation unterwandert, weil ein »diffus bedrohliches Gefühl des Beobachtetseins« zu Duckmäusertum führen und »eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann«. So formulierte es das Verfassungsgericht 2010[4]. Zum anderen wird das Vertrauen in den Rechtsstaat erschüttert, wenn nicht gar zerstört. »Verfassungspatriotismus« als identitätsstiftendes Element der Bundesrepublikaner, wie Jürgen Habermas es in den 80ern formulierte,

hätte ausgedient, wenn sich die Funktionsfähigkeit unseres Rechtsstaats zwar noch auf das Verteilen von Knöllchen für Falschparker, nicht aber mehr auf die Durchsetzung unserer Grundrechte erstreckte.

In der NSA-Affäre gerät derweil die Pressefreiheit massiv unter Druck: So verlangte und beaufsichtigte der britische Geheimdienst GCHQ, das Pendant zur National Security Agency im Vereinigten Königreich, beim »Guardian« im Juni die Zerstörung von Festplatten mit den Dokumenten Snowdens. Der Chefredakteur der Zeitung, Alan Rusbridger, warnte, dass die totale Überwachung eine grundsätzliche Gefahr für den Journalismus sei. Den Partner des Snowden-Vertrauten und Guardian-Autors Glenn Greenwald, David Miranda, hielten die Sicherheitsbehörden im August ferner neun Stunden am Flughafen fest und beschlagnahmten seine Computerausrüstung bei einem Zwischenstopp in London. Auch hier ist das Ziel des Einschüchterns der »4. Gewalt« unübersehbar.

Und ganz allgemein entsteht für Unternehmer/innen, Beschäftigte und Bürger/innen ein hohes Maß an Verunsicherung, welche Kommunikationskanäle sie noch sicher nutzen können. Wir müssen Antworten finden auf die Fragen, wie angesichts der bekannt gewordenen umfassenden Internetschnüffelei Wirtschaftsspionage verhindert sowie Arbeitnehmerdatenschutz und Koalitionsfreiheit verwirklicht werden können. Und wie die hochgradig vernetzten öffentlichen Verwaltungen in Bund, Ländern und Gemeinden sowohl untereinander als auch mit Bürger/innen und Unternehmen Daten austauschen können, ohne Gefahr zu laufen, dass diese überwacht oder gar manipuliert werden. Gleiches gilt insbesondere für den Gesundheits- und Bankensektor, aber auch etwa für den gesamten Bereich von Produktion und Dienstleistung.

Die Gefahr der digitalen Totalüberwachung ist nicht mehr Fiktion, sie ist bereits Realität. Und sie geht nicht nur von Geheimdiensten aus. Snowdens Enthüllungen haben gezeigt, wie verletzlich unsere IT-Infrastrukturen sind. Bisher hat die Politik sich nicht ihrer Verantwortung gestellt, klare gesetzliche Rahmenbedingungen für die Online-Welt zu schaffen, die sich an den Grundrechten und am

Verbraucher- und Datenschutz orientieren. Im Gegenteil, das Bundesinnenministerium etwa setzt seit Jahren bei Facebook & Co sowie beim Sichern der Privatsphäre gegenüber der Wirtschaft allgemein vor allem auf nebulöse Selbstverpflichtungserklärungen. Im Lichte der NSA-Affäre forderte Innenminister Hans-Peter Friedrich nicht etwa Aufklärung und Folgen von der US-Regierung, sondern verkündete ein vermeintliches »Supergrundrecht *Scherheit*«. Damit zeichnet sich das politische Ziel ab, Freiheitsrechte zu verschlechtern, statt sie zu stärken[5].

Schockwellen des NSA-Skandals

Aktuell wird in Unternehmen und Verwaltungen diskutiert, welche Hard- und Software einigermaßen Schutz vor Ausspähung bietet. Damit verknüpft ist die Frage, ob Produkte von Microsoft und Apple noch tragbar sind, wie es in dieser Hinsicht um die Hersteller aus dem asiatischen Raum bestellt ist und ob freie sowie quelloffene Technik nicht Standard sein sollte. Unklar erscheint vielen, welche ausländischen Online- und IT-Dienstleister man noch nutzen kann, wenn diese zur Herausgabe der Daten an ihre jeweiligen Geheimdienste angehalten werden können und letztere möglicherweise sogar Gesetzgebungen unterliegen, in denen explizit nicht nur die Terrorabwehr, sondern auch die Verfolgung ökonomischer Interessen Teil ihres Auftrags ist[6]. Schon aus Gründen eigener Wettbewerbsfähigkeit wäre es ratsam, wenn die entsprechenden Länder solche sehr weitgehenden Spionagebestimmungen abschafften.

Zuallererst ist Transparenz nötig, was Sicherheitsbehörden in traditionellen Demokratien erlaubt ist. In diesem Sinne forderten im Juli zahlreiche zivilgesellschaftliche Organisationen unter Einschluss des ver.di-Vorsitzendem und Bürgerrechtler in einem offenen Brief an die nationale und die EU-Ebene unter dem Motto »Stop Surveillance«[7], »alle Verträge, Gesetze und Maßnahmen unmittelbar offenzulegen«, welche die informationelle Selbstbestimmung der Bürger betreffen und diese möglicherweise verletzen. Internationale Kooperationen zwischen

Strafverfolgungsbehörden, Justiz und Geheimdiensten dürften nicht zur Umgehung des innerstaatlichen Grundrechtsschutzes missbraucht werden, heißt es in dem Schreiben gegen jede Form anlassloser und unverhältnismäßiger Überwachungsmaßnahmen weiter. In internationalen Verträgen müsse der Schutz und die Achtung der Privatheit sowie entsprechende Rechtsmittel auch gegen Überwachungsmaßnahmen durch Drittstaaten verankert werden.

Immerhin gibt es in den westlichen Ländern noch einen Rechtsstaat, auf den sich die Bürger beziehen können und der eine Kontrolle von Sicherheitsbehörden zumindest theoretisch erlaubt. In anderen Ländern der Welt und insbesondere in autoritären Staaten existieren rechtsstaatliche Normen entweder in geringerem Ausmaß oder lassen sich noch weniger durchsetzen. Gleichwohl ist davon auszugehen, dass deren Geheimdienste in ähnlicher Weise aktiv sind wie die der USA und Großbritanniens.

Reform rechtsstaatlicher Kontrolle und digitaler Selbstschutz

Es sind also zum einen Gesetze zu erlassen und Vereinbarungen auf möglichst globaler Ebene zu treffen, um die rechtsstaatliche Kontrolle über die in eine Parallelwelt entfleuchten Spionagegroßmeister wiederzuerlangen und funktionstüchtig zu gestalten. Dabei ist im Blick zu behalten, dass Firmen viel Geld damit verdienen, indem sie den Staat bei der Netzspionage unterstützen. Das macht parlamentarische Überwachungsgremien zur prominenten Zielscheibe für aggressiven Lobbyismus und Bestechungsversuche.

Zudem bleibt es wichtig, Möglichkeiten zum digitalen Selbstschutz etwa durch geprüfte Verschlüsselungsverfahren bekannter und einfacher zu machen. Die Aufklärung über die Gefahren von Datenverlusten und der Profilbildung ist sträflich vernachlässigt worden. Bürger, Jugendliche, Kinder wissen häufig wenig über die Grundfunktionen und Mechanismen des Netzes. Welche Werkzeuge zum Datenschutz werden ihnen angeboten? Welche Vorgaben macht der Verbraucherschutz? Werden diese kontrolliert und bei Missbrauch sanktioniert? Welchen

Kriterien unterliegt der Aufbau der öffentlichen Infrastrukturen des Staates und seiner Bürgerdienste?

Auch hier stecken oft IT-Lobbyisten ihre Claims ab und setzen allein auf Verfahren, mit denen ihre Firmen viel Geld verdienen können. Es fehlt dagegen an klaren Bestimmungen, welche Daten online verarbeitet werden dürfen und welche man tunlichst aufgrund der großen Missbrauchsgefahr aus der digitalen Welt heraushalten sollte. Dazu gehören etwa Krankheitsdaten; vielleicht ist das Netz im Lichte der Spionage-Enthüllungen aber auch nicht der richtige Ort für manche Verfahren im Bereich des E-Government und des Rechtswesens. Doch wer erstellt eine Liste, welche Dienste nicht übers Netz angeboten und welche (kritischen) Infrastrukturen keinesfalls ans Internet angebunden werden sollten?

Die Politik muss nachsitzen

Für Regierungen sind solche Fragen in der Tat oft noch »Neuland«. Die Politik hat es bisher nicht als ihre Aufgabe begriffen, sich selbst wirklich fachkundig zu machen und einen belastbaren und tragfähigen Rechtsrahmen für das Internet zu erarbeiten, der sich am Gemeinwohl orientiert. Sie hat das Feld stattdessen weitgehend den Unternehmen– und eben den Geheimdiensten – überlassen. Jetzt gilt es, die Online-Welt endlich als öffentlichen Raum zu verstehen[8].

Genauso muss die Politik das Internet von seiner technischen Seite her besser begreifen. »Code is law.« Mit diesem Satz hat der US-Rechtsprofessor Lawrence Lessig schon Ende der 1990er deutlich gemacht, dass Programme, Software, technische Architekturen und Standards auch rechtliche sowie soziale Normen setzen. Der Jurist wollte mit dieser Ansage vor allem der in den Anfängen des Internets weitverbreiteten Meinung entgegentreten, dass das weltweite Kommunikationsnetz nicht kontrolliert und reguliert werden könne, weil seine Grundstruktur dagegen immun sei. Positiv gewendet lässt sich sagen, dass es maßgeblich auch von politischen Entscheidungen abhängt, wie die Architektur des Netzes und anderer technischer Basisinfrastrukturen ausfällt. Regulierer legen fest, ob das Internet ein

Ort der Freiheit bleibt oder repressive Kontrolle schafft und ob es demokratische Strukturen sowie Rechte unterstützt oder torpediert.

Und es gilt, die spezifische Missbrauchsanfälligkeit der Online-Welt, die ungeheuerlichen Überwachungs- und Auswertungsmöglichkeiten und ihre Gefahren für den einzelnen Bürger, für jedes Unternehmen und die Demokratie als Ganzes zu verstehen. Snowdens Enthüllungen sind ein Weckruf für die Demokratie. Wir dürfen uns jetzt nicht die Ohren zuhalten, weil ein Gegensteuern mit – unangenehmer – Arbeit verbunden ist.

Jedes größere, für die Öffentlichkeit relevante IT-Projekt muss vielmehr der Prüfung unterzogen werden, ob es missbrauchsresistent und demokratiekompatibel – oder -schädlich ist. Der Verbraucher- und Datenschutz muss in die Planung von Alltagsgeräten und Infrastrukturen einbezogen werden. Notwendig ist eine Art demokratischer Technikfolgenabschätzung. Sie muss reichen von der elektronischen Gesundheitsakte über das neue Internetprotokoll IPv6 und »Smart Cities« bis hin zum »Internet der Dinge«, mit dem Überwachungstechnologien in die Alltagsgeräte unserer Wohnungen wie Fernseher und Fortbewegungsmittel eingebaut werden könnten. Gefordert ist ein neuer Gesellschaftsvertrag zum Sichern der Privatsphäre in der digitalen Welt, der sich der technikgetriebenen Entwicklung von Überwachungsstaaten Orwellschen Ausmaßes entgegenstemmt[9].

Noch sind auf dem Weg dorthin viele Fragen offen: Wer setzt die Standards? Haben wir die in Fragen von Technik und Gemeinwohl ausgebildeten Fachkräfte? Wie steht es um unsere Forschungsinfrastruktur? Gibt es noch unabhängige, gemeinwohlorientierte Forschung? Oder ist es nicht vielmehr so, dass aufgrund der Drittmittelabhängigkeit Unternehmensinteressen dominieren und über IT-Infrastrukturen ohne Bedenken umfassende, zu Profilen zusammenfügbare personenbezogene Daten gesammelt werden, da es sich dabei um die Währung des digitalen Zeitalters handelt? Wissen Führungskräfte und Entscheidungsträger/
innen im öffentlichen und privaten Bereich um die Dimensionen

möglicher technischer Abhängigkeit, routinemäßiger Auswert- und Manipulierbarkeit? Unabdingbar ist, dass die Bürger/innen die Hoheit über ihre Daten bewahren können müssen – ohne dass sie sich aus dem öffentlichen Leben zurückziehen.

Kernforderungen an eine grundrechtsbewusste Netzpolitik nach Snowden

Wir brauchen eine Task-Force »Digitale Demokratie«

Die Zeit drängt. Die Tücken und Lösungsmöglichkeiten bei der gemeinwohlorientierten Infrastrukturplanung müssen rasch aufgezeigt, bestehende und geplante IT-Projekte von öffentlicher Relevanz auf ihre Demokratieverträglichkeit hin evaluiert werden. Eine solche Arbeit darf nicht von IT-Lobbyisten, sondern muss von unabhängigen Fachkräften interdisziplinär ausgeführt werden. Das kostet Geld. Private Unternehmen und öffentliche Verwaltungen sollten diese Kosten in ihre Haushaltsplanungen aufnehmen. Die Erarbeitung von Kriterien für gemeinwohlorientierte IT-Infrastrukturen bedarf öffentlicher Transparenz.

Wir müssen um unsere Grundrechte kämpfen – national und international

Wir müssen um unsere Grundrechte kämpfen, sonst ist die Demokratie am Ende[10]. Es ist höchste Zeit für ein Wiedererstarken urdemokratischer Tugenden zur Verfassungstreue in den USA. Beim transatlantischen Freihandelsabkommen, das derzeit verhandelt wird, bedürfen die Fragen des Datenschutzes der Klärung. Dafür muss die künftige Bundesregierung umgehend neue Impulse in Washington und Brüssel setzen und über die bereits ins Spiel gebrachten Änderungen eines UN-Pakts die Sicherung der Privatsphäre endlich weltweit zum Menschenrecht erklären. Es ist überfällig, das informationelle Selbstbestimmungsrecht zum Exportschlager zu machen. Generell muss eine Gesellschaft demokratisch unter Abwägung aller Folgen entscheiden, welche Form der Überwachung sie akzeptieren und wie sie das Missbrauchspotenzial anhand klarer, nicht überschreitbarer Grenzlinien reduzieren will. Konzerne müssen an der pauschalen

Weitergabe von Daten an Drittstaaten etwa im Rahmen der »Safe Harbor«-Übereinkunft gehindert werden. Transatlantische Abkommen zum Transfer etwa von Finanz- oder Flugpassagierdaten gehören auf den Prüfstand.

Wir brauchen bessere Formen der informationellen Selbstverteidigung

Neben der politischen Arbeit müssen wir zur informationellen Selbstverteidigung greifen. Die Nutzung von Verschlüsselungsprogrammen und Anonymisierungsservern ist der nächste Schritt, den wir in unseren Alltag integrieren sollten. Die Technik bietet Möglichkeiten zum grundsätzlichen Schutz unserer Kommunikation gegen die Ausspähung von Dritten, aber keinen Rundumschutz. Nötig sind einfach zu nutzende Anonymisierungsserver und Verschlüsselungsprogramme, um zu verhindern, dass über jeden Nutzer umfangreiche Dossiers angehäuft werden können. Derzeit zieht jeder, der Kryptographie im Internet anwendet, aber erst recht das Interesse von Geheimdiensten auf sich. Nur mit weitreichenden Initiativen zum Selbstschutz und konsequentem Umstellen auf verschlüsselten Netzverkehr durch Diensteanbieter kann dies vermieden werden. Dabei ist starke Kryptographie vorzuschreiben; die eingesetzten Verfahren sind möglichst auf EU-Ebene in gründlichen Audits zu überprüfen, um Hintertüren für unerwünschte Horcher auszuschließen. Letztere führen zu allgemeiner IT-Verunsicherung, da nicht nur »die Dienste« solche gezielten Lücken und Verwundbarkeiten nutzen können.

Gefragt sind Bündnispartner, um die Selbstschutztechniken nutzerfreundlicher zu gestalten und den Verfahren zur Umgehung von Kryptographie, etwa durch Angriffe auf Betriebssysteme und Browser, zu begegnen. Hilfreich sind neben Unterstützern in der Politik auch Kontakte zu Unternehmen, die Wirtschafts- oder Forschungsspionage verhindern wollen oder die von der Einführung datenschutzfreundlicher Technik und Dienstleistungen profitieren. Verbraucherschützer sollten in Zukunft eine zentrale Rolle bei der Gestaltung von IT-Produkten und IT-Geschäftsmodellen spielen. Eingebunden werden in den Kampf für eine starke Verschlüsselung und

sichere digitale Technik können zudem Kryptographen, Investoren, Entwickler, Programmierer, Wissenschaftler und andere besorgte Nutzer[11].

Wir benötigen mehr dezentrale Netzinfrastrukturen

Datensparsamkeit in der Online-Welt hilft immer. Wer seine Kommunikation nicht reduzieren will oder kann sollte auf dezentrale Formen wie den eigenen E-Mail-Server setzen. Die Konzentration auf eine Handvoll großer Online-Plattformen macht diese zum besonders begehrten Ziel der Datenabzapfer. Die EU sollte Hosting-, Cloud- und Routingdienste für das eigene Territorium aufbauen, um von den USA unabhängiger zu werden. Auch drahtlose Nachbarschaftsfunknetze via WLAN, die eine direkte Kommunikation erlauben, werden als »Gegengift« zur Überwachung gesehen[12]. Freie Soft- und Hardware können helfen, IT-Infrastrukturen einfacher auf Schwachstellen und Hintertüren hin abzuklopfen. Die technischen Herausforderungen, die der Bespitzelungsskandal aufwirft, werden in der Netzgemeinde bereits offensiv und praktisch unter dem Motto »#youbroketheinternet – we'll make ourselves a new one« diskutiert. Dabei geht es um informationelle Selbstbestimmung und Datenhoheit sowohl in sozialen Netzwerken wie ganz allgemein um die Frage vertrauenswürdiger und sicherer Kommunikationswerkzeuge.

Wir brauchen einen besseren Schutz der Pressefreiheit und von Whistleblowern

Pressefreiheit und ein starker Quellenschutz müssen in einer Demokratie unantastbar sein. Sie gehören zum Kern westlicher Werte und zum System der »Checks and Balances«. Die USA und Großbritannien müssen auch ihren Kampf gegen Hinweisgeber beenden. Die Stellung von Whistleblowern ist national und international deutlich zu stärken, insbesondere dürfen von einschlägigen Schutzbestimmungen der Militär- und Geheimdienstbereich nicht ausgeschlossen werden. Nach dem internen Läuten der Alarmglocken in Institutionen muss Beobachtern von Missständen der Gang an die Öffentlichkeit erlaubt sein. Für eine breite Aufklärung über Fehlentwicklungen darf die Gesellschaft nicht nur auf Individuen bauen,

die große persönliche Opfer erbringen. Erforderlich sind eine starke Zivilgesellschaft mit entsprechender Courage sowie effiziente Kontrollgremien.

Dieser Text ist am 4. Oktober 2013 fertiggestellt worden.

Die Gedanken sind frei

Anne Roth

Hast du eigentlich irgendwas an deinem Verhalten geändert nach den Snowden-Leaks?

Meine erste Reaktion auf die Frage war anfangs »Nein«. Ich habe vorher schon E-Mails verschlüsselt, benutze Browser-Add-Ons gegen Tracking durch Unternehmen; ich weiß, dass Überwachung stattfindet. Seit Jahren nerve ich meine Umgebung mit Erklärungen, warum ich keine Post von Gmail-Accounts kriegen will: Weil bekannt ist, dass Google seine Services nicht verschenkt, sondern eine Gegenleistung erwartet, nämlich Informationen über die Nutzer/innen, und dazu auch in den Mails nach interessanten Details sucht. Inklusive der Informationen über die, mit denen korrespondiert wird, auch wenn die keine Mail-Accounts bei Gmail haben.

Wenn ich darüber nachdenke, merke ich, dass nicht ganz stimmt, dass sich nichts geändert hat. Ich verschlüssele wieder mehr. Nicht nur E-Mails, in denen Telefonnummern, Adressen oder andere persönliche oder politische Informationen stehen, von denen ich denke, dass sie niemanden etwas angehen, sondern auch E-Mails mit vollkommen banalem Inhalt. Auf mehreren meiner Mailinglisten wurde darum gebeten, dass Mail-Adressen bei den Providern, bei denen durch die Snowden-Leaks bekannt wurde, dass sie Daten an die NSA weitergeben, bitte durch andere ersetzt werden mögen. Gefolgt von der obligatorischen Debatte, welche Anbieter denn besser wären: lokale kommerzielle Anbieter, weil die Daten dann vielleicht nicht durch Unterseekabel sofort bei GCHQ und NSA landen? Lieber keine kommerziellen Anbieter, weil die im Zweifelsfall nicht mitteilen würden, dass eine Strafverfolgungsbehörde vor der Tür stand und wissen wollte, wer wem wann was geschickt hat, oder womöglich dem BND die Daten direkt weiterleiten, genauso wie es in den USA passiert? Nur welche mit Servern in Island? Oder doch in den USA, weil es da keine Vorratsdatenspeicherung gibt? Ein derzeit nicht aufzulösendes

Dilemma, weil wir nicht alles wissen und weil es keine gute Alternative gibt.

Natürlich gibt es kein Szenario, das vor allen denkbaren Gefahren schützt; das war schon vor den Leaks klar. Seit wir aber wissen, dass die Realität alle paranoiden Ideen lässig überholt, wissen wir etwas besser, dass wir mit etwas Aufwand zwar manchen Facetten der Überwachung begegnen können. Vor allem aber wissen wir, dass sehr viel mehr überwacht wird, als die es sich die meisten vorher vorstellen wollten.

Wenn Gartenbau verdächtig macht

Zurück zu meinem eigenen Verhalten: Ich merke, dass es einen Unterschied macht, ob ich nur *vermute*, dass jemand mitliest und nachschaut, für welche Websites ich mich interessiere, oder ob ich *weiß*, dass das geschieht. Es ist einfacher, die Vermutung zu verdrängen als das Wissen. Auch wenn es kein Mensch ist, der irgendwo sitzt und liest, ist jetzt klar, dass alles gespeichert und automatisiert durch ein Raster gezogen wird. Wie das Raster genau funktioniert, wissen wir nicht, aber dass zumindest Teile unserer Kommunikation betroffen sind, wissen wir schon. Es wird nach Auffälligkeiten gesucht; nach allem, das sich vom normalen Kommunikationsverhalten unterscheidet. Von meinem normalen Kommunikationsverhalten und vom allgemein üblichen Kommunikationsverhalten.

Verschlüsselte E-Mails werden länger aufgehoben, denn die sind verdächtig. Wenn ich mit bestimmten Menschen regelmäßig verschlüsselte E-Mails austausche und zwischendurch ausnahmsweise nicht, ist das möglicherweise auch verdächtig. Zumindest auffällig. Als Methode ist das nicht neu, aber neu ist, dass alle davon betroffen sind. Ich spüre also bei allem, was ich tue, dass mir jemand Unsichtbares über die Schulter sieht und denke darüber nach, ob ich bestimmte Websites wirklich aufrufen sollte. Ich lasse mich letzten Endes nicht davon abhalten, aber der Gedanke taucht manchmal auf. Was sind Auffälligkeiten in meinem Verhalten? Wenn ich plötzlich nach Gartenbau-Geschäften suche, obwohl ich keinen Garten habe und mich noch nie dafür interessiert habe? Oder wenn ich drei Artikel über

Brandanschläge auf die Berliner S-Bahn lese und ein paar Tage vergesse, die Tabs im Browser wieder zu schließen? Können die sehen, dass ich meistens mit Google suche, aber manchmal auch nicht? Und was?

An diesem Punkt angekommen denke ich, dass ich damit aufhören sollte, Paranoia zu entwickeln. Ich bin keine muslimische Fundamentalistin und es ist unwahrscheinlich, dass ich versehentlich für eine gehalten werde. Für Aktivistinnen außerhalb der USA und Großbritannien interessieren sich NSA und GCHQ nicht besonders, und die deutschen Behörden wissen in etwa, was ich so mache. Das hilft nicht immer, schon klar, aber für die meisten stimmt es schon. Für alle aus arabischen Ländern oder mit arabischen Namen allerdings sieht es schon wieder anders aus.

Viele fühlen sich also nicht wirklich persönlich bedroht. Wir sind nicht die Terroristen, die sie suchen. Und weil alle überwacht werden, verschwinden wir irgendwie in der Masse. Es ist unvorstellbar, wie aus der Datenmenge etwas entstehen kann, das tatsächlich mich persönlich gefährdet. Dazu kommt, dass die Totalität der Überwachung und die Menge der (demokratisch legitimierten) Behörden, die darin verstrickt sind, schwer zu begreifen sind.

Bedrohlicher ist die Massenüberwachung auf einer abstrakteren Ebene für Menschen, die sich mit dem Alltag von Strafverfolgungsbehörden oder Geheimdiensten beschäftigen, für die, die besser verstehen, welche Macht in technischen Systemen liegt und für die, die sich Gedanken über politische Systeme und die Idee der Demokratie machen.

Weniger bedrohlich ist sie für Menschen, die andere, spürbarere Probleme haben; weil sie von der Wirtschaftskrise betroffen sind – viele Menschen in anderen europäischen und nicht-europäischen Ländern – oder weil sie viel direktere Formen von Überwachung erleben, z.B. Trojaner-Viren, die von Regierungen gegen die Opposition eingesetzt werden.

Wer beobachtet wird, ändert das Verhalten

Ein zentrales Problem der Überwachung für alle ist, dass wir unser Verhalten ändern, wenn wir wissen, dass wir beobachtet werden. Das ist vielfach erforscht und beschrieben worden. Damit erleben wir eine direkte Einschränkung von elementaren Freiheiten und Grundrechten, in erster Linie der Meinungsfreiheit. Das wirkt sich auf alles aus, was wir öffentlich sagen oder schreiben und natürlich auch auf Situationen, von denen wir annehmen, dass sie nicht-öffentlich sind: etwa private E-Mails und Gespräche, nicht-öffentliche Websites oder auch alle scheinbar durch Privacy-Einstellungen geschützten Online-Plattformen wie Facebook oder Flickr. Wenn wir aber nirgends den Raum haben, frei zu sagen oder zu schreiben, was wir denken und damit auch keinen Raum haben, Gedanken zu entwickeln, zu testen und zu überprüfen: Wieviel Freiheit bleibt dann noch?[13]

Ich weiß das alles und habe dennoch den Eindruck, dass sich an meinem Verhalten nicht viel ändert. Ein bisschen mehr Verschlüsselung, ein bisschen weniger Google-Suche. Ich schalte mein Smartphone öfter aus und achte darauf, dass es nicht den ganzen Tag auf meinem Schreibtisch liegt. Die Kamera an meinem Laptop war vorher schon abgeklebt, seit den Leaks lege ich auch etwas auf die Kamera meines Telefons. Ich schreibe meistens, was ich für richtig halte.

Andererseits: Wie wäre es, wenn ich sicher sein könnte, dass wirklich niemand mitläse? Bzw. meine (mehr oder weniger) öffentlichen Texte auf mögliche terroristische, kritische, auffällige Inhalte überprüfte und in unbekannte Kategorien von Geheimdienst-Datenbanken einsortierte?

Eine weitere Auswirkung sind die vielen Gespräche mit Leuten, die jetzt gern verschlüsseln würden, aber nicht wissen, wie. Dann kam die Nachricht, dass auch Verschlüsselung geknackt werden kann. Danach Gespräche darüber, ob das stimmt, in welchen Fällen das stimmt und wen das betrifft.

Mit »E-Mail made in Germany« wollen Telekom, WEB.DE und GMX sichere E-Mail anbieten[14], aber was heißt eigentlich sicher? Was meinen sie mit »verschlüsselt«? Oder ist das den Leuten nicht sowieso egal, weil die sich nur kurz beruhigen und dann wieder mit was

anderem beschäftigen wollen? Macht es Sinn, damit anzufangen, Leuten das Verschlüsseln beizubringen, wenn sie sich letztlich doch nicht von ihrer Webmail trennen werden und alles andere zu kompliziert finden, um es regelmäßig in ihren Alltag zu integrieren? Besser wäre, dazu beizutragen, dass die nötigen Werkzeuge einfacher zu benutzen sind. Trotzdem wird es sie nicht heute und auch nicht im nächsten Monat geben.

Die Liste der Sachen, die ich mir genauer durchlesen will, damit ich besser verstehe, worauf es bei bestimmten Sicherheitsmaßnahmen ankommt, wächst. Immerhin ist es beruhigend, zu sehen, dass Krypto-Expert/innen aller Gewichtsklassen ständig diskutieren, worauf es wirklich ankommt und sich selten einig sind, was der beste Schutz ist: Das zeigt, dass es fast unmöglich ist, alles richtig zu machen. Gleichzeitig auch beunruhigend, denn die andere Seite wirkt doch ziemlich entschlossen.

Ausgehend von dem Wissen, dass es auch digital keine absolute Sicherheit gibt, bin ich schon länger der Meinung, dass es auf jeden Fall sinnvoll ist, so viel wie möglich zum eigenen Schutz zu tun. Es ist ja auch kein großes Problem, Türschlösser zu knacken und wir schließen trotzdem hinter uns ab, in der Hoffnung, dass das zu erwartende Gefummel mögliche Einbrecher/innen eher abhält als eine weit offen stehende Tür.

Nichts zu verbergen

Früher oder später taucht jemand auf, der oder die nichts zu verbergen hat. Schon gar nicht vor der NSA oder anderen Geheimdiensten. Für diesen Fall sitzt locker in der Hosentasche ein kleines Set an Argumenten:

- die Leute, die in Mails oder in ihren Facebook-Profilen missverständliche Scherze gemacht haben und deswegen nicht in die USA einreisen durften oder gleich festgenommen wurden
- die Leute, denen etwas Ähnliches in Europa passiert ist

- die Leute, die lieber nicht wollten, dass Arbeitgeber/in oder Familie von der Abtreibung oder Affäre erfahren
- der Stalker
- die Steuererklärung
- Firmen-Interna
- der Unterschied, ob ich freiwillig entscheide, Informationen über mich weiterzugeben oder ob ich dazu gezwungen werde

Auf der anderen Seite gibt es die, die lakonisch bis überheblich erklären, dass das alles nichts Neues sei, dass sich nichts Relevantes getan hat und deswegen auch keine Notwendigkeit besteht, irgendetwas zu ändern.

Ja, wir wussten von Echelon[15] und wir wussten auch durch die früheren Whistleblower, dass die NSA in Utah einen großen Datenspeicher baut. Eins der beliebtesten Gesprächsthemen im Bereich Computersicherheit ist die Fachsimpelei, wie viel Rechenkapazität nötig ist, um Schlüssel dieser oder jener Länge zu knacken und wie lange das dauern wird. Selten kommt in diesen Gesprächen die Frage vor, was das jeweils kostet und ob Behörden bereit und in der Lage sind, die entsprechenden Ressourcen einzusetzen. Meiner Meinung nach ist die Option, dass etwas in x Jahren geknackt werden kann, das beste Argument dafür, so viel wie möglich zu verschlüsseln, auch wenn ich davon ausgehe, dass möglicherweise in 10 Jahren diese oder jene Mail von mir gelesen wird. Denn je mehr verschlüsselt ist, desto mehr sinkt auch die statistische Wahrscheinlichkeit, dass meine Mails bei denen dabei sind, die tatsächlich entschlüsselt werden.

Und Google Earth?

Schließlich gibt es regelmäßig Diskussionen, die sich darum drehen, dass sich viel zuwenig Menschen dafür interessieren, was die Snowden-Leaks ans Licht gebracht haben. Warum gibt es in Deutschland einen Aufstand, wenn Google-Autos Häuser fotografieren, aber nicht, wenn Inhalte und Meta-Daten unserer gesamten digitalen Kommunikation überwacht werden?

Die einfache Interpretation ist, dass die Menschen eben einfältig sind und dazu von tiefsitzendem Anti-Amerikanismus beseelt. Ich halte das für falsch und zudem arrogant. Falsch, weil nicht überraschend ist, dass etwas, das sichtbar und dessen Auswirkungen damit vorstellbar sind (die Google-Autos und die Bilder der Häuser im Netz), viel mehr Angst erzeugt als die völlig abstrakte Überwachung durch NSA, GCHQ und womöglich auch den BND.

Arrogant ist es, weil wir auf demokratische Weise nur dann etwas ändern können, wenn viele etwas ändern wollen. Wir müssen nicht alle einer Meinung sein, aber wir müssen am selben Strang ziehen. Aus den beschriebenen Gründen gibt es weniger Angst vor Überwachung als angemessen wäre, aber wenn es sie gibt, dann müssen wir das nutzen, um politisch etwas zu ändern. Genauso ist es unser Job, das Abstrakte und schwer Vorstellbare an der Überwachung, die wir jetzt sehen, besser zu erklären und vorstellbar zu machen. Und unser Wissen darüber zu teilen, wie wir uns dagegen schützen können. Natürlich ist es ein Problem, dass so viele Menschen viele Informationen scheinbar freiwillig an die Unternehmen weitergeben, die direkt mit den Geheimdiensten kooperieren. Mindestens genauso so problematisch ist aber, dass das Wissen darüber, wie digitale Kommunikation und technische Netzwerke funktionieren, für viele immer noch eine Art Geheimwissen ist.

Wenn sich alle trauten, ihre scheinbar dummen Fragen zu stellen, wären wir einen großen Schritt weiter.

Die neuen Krypto-Kriege

Constanze Kurz, Frank Rieger

Das Angebot, das der texanische Dienstleister Lavabit seinen Kunden machte, war in Hinsicht auf die NSA-Diskussionen der letzten Monate ausgesprochen zeitgemäß: E-Mails wurden auf dem Server verschlüsselt gespeichert, nur der Empfänger konnte mit seinem Passwort darauf zugreifen. Zu den Kunden zählte Edward Snowden, als Geheimdienstmitarbeiter mit der Notwendigkeit, die eigene Kommunikation zu schützen, überaus vertraut.

Doch der Kunde Snowden wurde Lavabit zum Verhängnis. Seit schon kurz nach Beginn seiner NSA-Enthüllungen bekannt wurde, dass er seine E-Mails bei diesem Anbieter speicherte, dürften die Geheimdienste dort vorstellig geworden sein. Laut den Angaben des Lavabit-Gründers Ladar Levison folgte ein wochenlanges juristisches Tauziehen – das er am Ende verlor.

Der Dienst zog jetzt die Notbremse und stellte sein Angebot kurzerhand vollständig ein. Ein ebenso drastischer wie konsequenter Schritt: Levison schrieb, er wolle kein Komplize werden bei Verbrechen an der amerikanischen Bevölkerung. Sein Unternehmen beruhte schließlich auf dem Versprechen sicherer Kommunikationsinfrastruktur.

Die neuesten Opfer der außer Rand und Band geratenen Geheimdienst-Clique sind also kleinere amerikanische Anbieter, die sich den Verfassungsgrundsätzen verpflichtet fühlen, sowie als Kollateralschaden die zehntausenden privaten und ein paar dutzend Unternehmen als Kunden von Lavabit. Ein weiterer amerikanischer Anbieter, der ein ähnliches Produkt offerierte, stellte einen Tag später ebenfalls seinen E-Mail-Dienst ein. Man wolle sich nicht in eine Situation bringen, in der man zwischen der Loyalität zu den Nutzern und den Forderungen des Staates entscheiden müsse.

Die Details der Forderungen an Lavabit sind geheim. Da die Firma in der Vergangenheit in Einzelfällen durchaus bei legitimen Strafverfolger-

Anfragen kooperiert hat, muss es wohl ein weitreichendes, die üblichen Prozeduren weit übersteigendes Ansinnen der Geheimdienste gewesen sein, das Lavabit zuerst zum juristischen Widerstand und dann zur Aufgabe bewegte. In solchen Fällen könnte ein »National Security Letter« erwirkt worden sein, der jegliche Preisgabe der Umstände an die Öffentlichkeit strikt verbietet, oder ein Beschluss des FISA-Geheimgerichts ergangen sein, der ebenfalls zu Stillschweigen zwingt.

Durch die Mechanismen, die nach dem 11. September mit dem »USA PATRIOT Act«, den FISA-Geheimgerichten und weiteren Ermächtigungen für schrankenlosen Zugriff etabliert wurden, können FBI, NSA & Co. Kommunikationsanbieter und Internetdienste quasi auf dem kleinen Dienstweg zur Kooperation nötigen. Juristische Gegenwehr ist praktisch nie erfolgreich, alles ist geheimzuhalten, womit es auch unmöglich ist, sich Unterstützung in der Öffentlichkeit zu holen. Geheime Schnüffelanordnungen, die auch ohne Richterbeteiligung erteilt werden können, mit geheimgehaltenen Begründungen, können nur vor Geheimgerichten angefochten werden – und die Betroffenen dürfen nicht einmal darüber reden. Das alles geschieht natürlich im Namen der Sicherheit vor dem Terrorismus – dem universellen Totschlagargument zur Aushebelung normaler Rechtsstaatsprozeduren.

Die Causa Snowden wird somit mehr und mehr zum Moment, in dem die Masken fallen und der »deep state«, wie die Washington Post den gigantischen Sicherheitsapparat in den USA getauft hat, seine wahres Gesicht zeigt. Denn das Verhalten gegen Lavabit rückt verdächtig nahe an Erpressung und Nötigung. Die Konturen, die immer mehr sichtbar werden, lassen erahnen, dass die Grundsätze der freiheitlichen Gesellschaft, die einst in der Verfassung der USA niedergelegt wurden und die nach dem Krieg auch ihren Niederschlag im westdeutschen Grundgesetz fanden, auch für Inländer nicht mehr viel gelten.

Nach CIA-Foltergefängnissen, massenweisen, noch immer anhaltenden Drohnen-Morden und mit auf nachgewiesenen Lügen begründeten Kriegen, die aber fern der Heimat stattfinden und für den normalen US-Bürger gut zu ignorieren sind, ist die Grundrechtsabschaffung im

Namen der Sicherheit nun ganz spür- und sichtbar zuhause angekommen.

Das Interessante daran ist: Im Falle Snowden geht es nicht einmal um die Sicherheit vor Terroristen. Es geht um schnöde Rache der Geheimdienste an einem Abtrünnigen, der es gewagt hat, etwas Licht hinter den Vorhang der Geheimniskrämerei zu werfen. Zu begründen, die Verfolgung von Snowden würde das Land sicherer machen, bedarf schon abenteuerlicher Rabulistik, vor der Friedensnobelpreisträger Barack Obama und seine Mannen aber auch nicht zurückschrecken.

Am Dienstag und am Donnerstag derselben Woche, in der Lavabit aufgab, traf sich der US-Präsident höchstselbst mit den Chefs der amerikanischen High-Tech-Branche: Apple, AT&T, Facebook, Yahoo, Microsoft und Google. Einige Bürgerrechtsorganisationen durften ebenfalls teilnehmen. Es wurde dem Vernehmen nach über die technische Überwachung gesprochen. Genaueres wurde allerdings nicht bekannt, denn die Treffen fanden unter Ausschluss der Öffentlichkeit statt.

Wir sind es ohnehin langsam gewöhnt, erst aus der Zeitung zu lernen, was wirklich in den amerikanischen Unternehmen gespeichert, ausgeleitet und dann von den Geheimdiensten ausgewertet wird. Keine der betroffenen Regierungen hat zur Aufklärung der tatsächlichen Details der geheimdienstlichen Vorgänge auch nur ein Bit beigetragen. Vielleicht wird in den Krisentreffen im Weißen Haus offen geredet, wie weit die US-Unternehmen den Geheimdiensten technisch entgegenkommen.

Den großen Datenspeicher-Unternehmen war offenkundig die erzwungene Geheimhaltung ganz recht, konnten sie sich doch vor ihren Nutzern hinter wolkigen Klauseln verstecken: »Wir arbeiten im Einzelfall wie gesetzlich vorgeschrieben mit Strafverfolgern zusammen.« Erst als durch die Snowden-Enthüllungen das Ausmaß der »Einzelfälle« und die gut geölten technischen Schnittstellen für die Datenübermittlung an die Dienste klar wurden, wollten Google, Microsoft & Co. plötzlich etwas mehr Transparenz in das Procedere

bringen. Aber natürlich auch nicht zu viel, das könnte die Kunden verschrecken.

Dass die Branchenriesen dem Präsidenten mit der Einstellung ihrer Dienstleistungen nach dem Vorbild Lavabit gedroht haben könnten, darf als ausgeschlossen gelten. Googles Geschäftsmodell würde nach Bekunden von Firmenvertretern schlicht nicht funktionieren, wenn die Nutzerdaten auf seinen Servern so gespeichert wären, dass die Firma sie nicht auswerten könnte.

Obwohl einige der US-Firmen mehrfach versucht haben, gerichtlich gegen die in den letzten Jahren in mehreren Schritten erweiterten Abhörmethoden vorzugehen: Die Krisengespräche dürften eher dem Umstand geschuldet sein, dass in der amerikanischen Wirtschaft so langsam die Angst umgeht. Die Cloud-Dienste, bei denen US-Unternehmen bislang unangefochtene Marktführer sind, verspüren einen erheblichen Einbruch von Nachfragen und Umsatz aus Europa und Asien. Das Vertrauen, dass die Daten dort schon sicher seien, ist dahin und wird so schnell auch nicht wiederherzustellen sein.

Die Warnung des Lavabit-Gründers in seiner Mitteilung über die Einstellung seiner Firma ist jedenfalls klar und eindeutig: Unter US-amerikanischer Jurisdiktion Dienste mit Privatsphären-Garantie anbieten zu wollen, ist schlicht nicht mehr möglich. Zu groß ist die Datengier der Geheimdienste, zu weitreichend ihre legalen Mittel und sonstigen Hebel, um sich den Zugriff zu erzwingen.

In den 1990er Jahren war der offensichtliche Versuch, kryptographische Verfahren zur Privatsphärenwahrung durch vorgeschriebene Hintertüren zu umgehen, gescheitert – die sogenannten Crypto Wars. Nun wird das gleiche Ziel durch juristische Knochenbrecher-Taktiken zur Knebelung und Verpflichtung der amerikanischen Internet-Anbieter erreicht, auf deren Sicherheitsversprechen sich die meisten Nutzer verlassen.

Der alte Kampf der Geheimdienste gegen die Verschlüsselung, die ihren Anspruch einschränkt, jede Kommunikation lesen und auf alle Daten zugreifen zu können, ist in eine neue Phase getreten. Die »Crypto Wars

2.0« werden mit geheimen Abhör-Anordnungen, mit geheimdienstlichem Hacking und dem Einsatz von Trojanern ausgefochten. Auf der Strecke bleiben Privatsphäre und Rechtsstaat, geopfert auf dem Altar eines nebulösen Sicherheitsversprechens, das nur noch das Feigenblatt zur Machterhaltung der Geheimdienste ist.

Erschienen am 10. August 2013 im Feuilleton der Frankfurter Allgemeinen Zeitung[16]*.*

NSA-Affäre: Der letzte Informant

Richard Gutjahr

Welche Folgen haben Überwachungsprogramme wie PRISM, Tempora und XKeyscore für den Journalismus? Müssen Journalisten ihre E-Mails künftig verschlüsseln, abhörsichere Handys benutzen? Und: Wie steht es um die Balance zwischen Staatsgewalt und Pressefreiheit? Richard Gutjahr hat mit zahlreichen Journalisten im In- und Ausland gesprochen und eine große Verunsicherung in der Branche ausgemacht.

> *»Nimm die Hintertreppe, wenn Du zu einem Treffen gehst. Nimm nicht dein Auto, sondern ein Taxi. Fahr zu einem Hotel, an dem nach Mitternacht noch Taxis warten. Nimm ein zweites Taxi, das dich nach Rosslyn bringt. Geh die letzten Häuserblocks zu Fuß. Wenn du verfolgt wirst, geh nicht in das Parkhaus. Ich weiß schon Bescheid, wenn du nicht kommst.«*[17]

Der Mann, der diese Anweisungen gab, wusste, wie er seine Spuren zu verwischen hatte – es war sein Beruf. William Mark Felt, stellvertretender Direktor des FBI zu Zeiten der Watergate-Affäre. Sein Spezialgebiet: die Spionageabwehr der Deutschen im Zweiten Weltkrieg. In die Geschichts- und Lehrbücher für Journalisten ist Felt aber unter einem anderen Namen eingegangen, unter der Bezeichnung jenes mysteriösen Informanten, der US-Präsident Nixon das Amt kostete: »Deep Throat«.

Eine rote Fahne im Blumentopf hinter dem Haus, zwei handgekritzelte Zeiger auf Seite 20 der New York Times, um die Uhrzeit für das nächste Treffen mitzuteilen. Spätestens seit PRISM und Tempora erscheinen die Methoden, mit denen Reporter-Legende Bob Woodward und Deep Throat miteinander kommuniziert hatten, geradezu als rührend.

40 Jahre nach Veröffentlichung des Watergate-Skandals wäre ein solches Treffen, trotz aller Vorsichtsmaßnahmen, vermutlich binnen weniger Stunden Ermittlungsarbeit aufgeflogen. Die Tiefgarage am

Wilson Boulevard in Rosslyn County, Virginia, wird heute videoüberwacht. Die GPS-Daten der Taxis, um dorthin zu gelangen, auf unbestimmte Zeit gespeichert und damit rekonstruierbar.

Die Enthüllungen der NSA-Spionageprogramme durch Edward Snowden lassen vieles, was wir vor kurzem noch als selbstverständlich angesehen haben, in neuem Licht erscheinen. Die Souveränität der Bundesrepublik Deutschland, das Recht auf Privatsphäre, die Pressefreiheit. Die informationelle Selbstbestimmung, laut Hans-Peter Uhl, innenpolitischer Sprecher der Union im Bundestag, eine »Idylle aus längst vergangenen Zeiten«?

»Mobiltelefone, Glasfaserkabel, PCs und den Internetverkehr, zu denen sich die NSA Zugang verschafft, gab es in der Blütezeit der Stasi noch gar nicht«, schreibt Daniel Ellsberg in seinem vielbeachteten Kommentar in der Washington Post mit dem Titel »United Stasi of America«. Der Whistleblower der Pentagon-Papiere zieht damit einen Vergleich, den Bundespräsident Joachim Gauck noch im ZDF-Sommerinterview entschieden ablehnte: »Wir wissen zum Beispiel, dass es nicht so ist wie bei der Stasi und dem KGB, dass es dicke Aktenbände gibt, in denen unsere Gesprächsinhalte alle aufgeschrieben und schön abgeheftet sind. Das ist es nicht.« Gauck vertraut seinem Freund, einem anderen ehemaligen Bürgerrechtler und späteren Präsidenten: Barack Obama.

Die Datenjournalisten von OpenDataCity wollten die Aussagen des Bundespräsidenten so nicht stehen lassen und programmierten eine interaktive Landkarte, nach der die Zettabytes an NSA-Daten, ausgedruckt in Aktenschränken, eine Fläche von ganz Europa einnehmen würden. »Die technischen Möglichkeiten von heute wären der feuchte Traum der Stasi gewesen«, so die aus der ehemaligen DDR stammende Piraten-Politikerin Anke Domscheit-Berg in der Talkshow Maybritt Illner.

Wenn Angela Merkel in diesen Tagen von der Balance zwischen Sicherheit und Freiheit spricht, dann sind es oft Journalisten, die den Behörden mit ihren Recherchen in die Quere kommen. Reporter, die

ihren Informanten als Schutzschild gegen staatliche Willkür und Amtsmissbrauch dienen. Doch mit der voranschreitenden Digitalisierung unseres Leben und einer ausufernden Datensammelwut des Staates werden diese Schutzschilde löchrig. Es stellt sich die Frage: Wie steht es eigentlich um die Balance zwischen Staatsgewalt und Pressefreiheit?

Noch bevor Edward Snowden das Flugzeug nach Hong Kong bestiegen hatte, erschütterte ein anderer, fast schon vergessener Skandal die Medienlandschaft: der gezielte Lauschangriff der US-Regierung auf Journalisten der Associated Press. Mindestens 20 Telefonanschlüsse, darunter auch die privaten Leitungen einiger AP-Mitarbeiter, wurden vom Justizministerium abgehört, um einen Informanten in der Bengasi-Affäre ausfindig zu machen.

Edward Snowden, Bradley Manning, John Kiriakou (ein ehemaliger CIA-Analyst, der das Waterboarding publik machte und dafür heute im Gefängnis sitzt) – nach Aussage des früheren NSA-Mitarbeiters Thomas Drake geht die Obama-Regierung bei ihrer Jagd auf Whistleblower noch unnachgiebiger vor als George W. Bush und alle seiner Vorgänger. Journalisten, die mit Whistleblowern reden, geraten selbst ins mediale Kreuzfeuer, werden in der Öffentlichkeit als Staatsfeinde oder Beihelfer von Terroristen gebrandmarkt. So ließ sich der New York Times-Kolumnist Andrew Sorkin in einem TV-Interview zu der Aussage hinreißen, er würde den Guardian-Journalisten Glenn Greenwald für dessen Komplizenschaft mit Snowden am liebsten gleich mitverhaften. Amerika habe derzeit keine funktionierende Demokratie, bringt es der frühere US-Präsident Jimmy Carter auf den Punkt.

Eine bei Weitem noch größere Bedrohung als die tatsächliche Verfolgung von Informanten sei der sogenannte »Chill Faktor«, warnt der Medienprofessor und Bestsellerautor Jeff Jarvis (»What would Google do?«) gegenüber dem »journalist«. Die Informanten würden sich zunehmend zurückhalten, aufgrund dieses »Kriegs gegen die Whistleblower«. Ähnlich sieht das auch die Hamburger Medienanwältin Dorothee Bölke: »Mit dem Vertrauensverlust gehen uns die Informanten

verloren. Die Informanten sind aber notwendig für eine funktionierende Presse in einem freiheitlichen Rechtsstaat.«

Jeff Jarvis tut sich schwer, den Schaden zu quantifizieren, denn wer auf brisanten Informationen sitzt, verhalte sich still. »Selbst wenn sich jemand ein Herz fasse, um mit einem Journalisten zu reden, ist die Kontaktaufnahme sehr viel komplizierter geworden, zumindest, wenn man es halbwegs sicher machen will.« Es erscheint paradox: Durch die digitale Kommunikation war es noch nie so leicht, mit Journalisten in Kontakt zu treten – und noch nie so schwer. Das Problem: »Wenn wir Mist bauen und eine unserer Quellen auffliegt, dann wird niemand mehr mit uns reden – ein Teufelskreis«, so Jarvis.

Müssen investigative Journalisten künftig ihre Mails verschlüsseln? So wie einst Deep Throat dem Washington-Post-Reporter Bob Woodward präzise Anweisungen für ihre Kommunikation gab, musste auch Edward Snowden seinem Kontaktmann beim Guardian zunächst einen Crashkurs in Verschlüsselungstechniken geben. »Verschlüsselung funktioniert«, so der ehemalige NSA-Mann auf die Frage eines Lesers im Guardian-Livechat. Richtig angewandt sei sie sogar äußerst zuverlässig. Dann räumt Snowden allerdings ein: Das eigentliche Problem sei die Ende-zu-Ende-Verschlüsselung.

Jürgen Kuri, stellvertretender Chefredakteur der Computerzeitschrift c't, erklärt: »E-Mails muss man sich wie Postkarten vorstellen, die jeder lesen kann. Verschlüsselte E-Mails sind Postkarten, die man vor dem Versenden in einen Briefumschlag gesteckt hat.« Auch die ließen sich heimlich öffnen, nur der Aufwand sei für die Mitleser eben deutlich größer. »Gegen professionelle Technologien eines Geheimdienstes haben wir keine Chance«, relativiert Georg Mascolo, der als SPIEGEL-Journalist und ehemaliger Chefredakteur schon über unzählige Spionage-Skandale berichtet hat. »Wir sind keine Geheimdienste. Wir sind Journalisten.«

Auf die Frage, weshalb die Süddeutsche Zeitung noch keine Möglichkeit anbiete, verschlüsselte Mails zu empfangen, antwortet Stefan Plöchinger, Chefredakteur von sueddeutsche.de: »Ich habe in mehreren Projekten die Erfahrung gemacht, dass Sicherungsinstrumente versagt

haben, ohne da präziser werden zu können. Meine Lehre war: Wenn ich Menschen etwas vermeintlich Sicheres öffentlich empfehle, zum Beispiel auf einer Toter-Briefkasten-Seite im Internet, fühlen sie sich dadurch vermutlich sicherer, als ich es ihnen garantieren kann.«

Auch Ronen Bergman, Geheimdienst-Experte bei der israelischen Tageszeitung Yedi'ot Acharonot, ist skeptisch. Man könne niemals wirklich sicher sein, dass die Verschlüsselungstechnologie, die man gerade benutzt, nicht schon lange geknackt ist. So hätten die Leute beispielsweise lange geglaubt, die Kommunikation über Skype sei sicher. »Snowden zeigt uns jetzt das genaue Gegenteil«. Selbst wenn eine Nachricht sicher verschlüsselt ist, könnte man noch immer einen Trojaner auf den Rechner spielen. »In dem Moment, in dem du die Mail öffnest und dechiffrierst, ist sie auch für deine Überwacher lesbar.«

Was den Schutz ihrer Quellen betrifft, sind Journalisten gesetzlich abgesichert durch das Zeugnisverweigerungsrecht. Doch was, wenn Journalisten in Zukunft gar nicht mehr nach ihren Quellen befragt werden müssen? Man stelle sich eine SPIEGEL- oder Cicero-Affäre vor, unter Zuhilfenahme der heutigen Technologie. Dorothee Bölke, die selbst mehrere Jahre als Justiziarin im SPIEGEL-Verlag gearbeitet hat, warnt: »Es gab Fälle, bei denen Strafbehörden unter Vorwand der Verletzung von Dienstgeheimnissen, Redaktionsräume durchsuchen ließen, um in diesem Zusammenhang auf Informationen über Kontakte und Quellen zu stoßen, die mit dem eigentlichen Durchsuchungsgrund gar nichts zu tun hatten.«

Die Algorithmen, mit denen die Stecknadel im Full-Take-Heuhaufen gefunden werden kann, werden immer effektiver. »Wenn gerade der E-Mail-Verkehr nach politisch sensiblen Stichworten gefiltert wird«, so die Medienrechtlerin Dorothee Bölke, »dann sehe ich da die Gefahr, dass gerade Journalisten ins Raster der Überwachung fallen.« Ob investigativer Reporter, Jurist oder Chefredakteur, wen immer man zu den Snowden-Enthüllungen befragt, man spürt eine große Verunsicherung. Und das ausgerechnet in einer Branche, die sonst selten verlegen ist um einen Kommentar. »Wir wissen nicht, was davon tatsächlich genutzt wird«, so der Computer-Experte Jürgen Kuri. »Noch

weniger wissen wir, was alles mit diesen Daten in fünf Jahren gemacht werden kann.«

Also doch besser zurück zur analogen Kommunikation? Nach einem Bericht der russischen Zeitung Iswestija setzt der Föderale Schutzdienst Russlands seit kurzem angeblich wieder verstärkt auf Schreibmaschinen. Besonders beliebt bei den Spionen sei das deutsche Modell Triumph-Adler Twen 180. Jürgen Kuri vom Computermagazin c't bringt es auf eine einfache Formel: »Sicher ist gar nichts.« Man könne nur versuchen, es seinen Überwachern so umständlich und so teuer wie möglich zu machen, sie auf diese Art und Weise zu einer Art »Kosten-Nutzen-Abwägung« zu zwingen. »Das ist die einzige Möglichkeit, die ich da momentan sehe.«

»Ich gehöre zu denen, die in der Lage wären, meine E-Mails selbst zu verschlüsseln«, sagt der WDR-Journalist Ranga Yogeshwar. »Aber wenn ich das täte, wäre das eine Kapitulationserklärung der Demokratie«. Der TV-Moderator empört sich darüber, dass seit den Snowden-Enthüllungen in den ARD-Talkshows zur Hauptsendezeit lieber über Themen wie »Rente«, der »Aldi-Check« oder »Schlaglöcher in deutschen Straßen« diskutiert werde. »Die Logik dahinter ist, dass diese Themen populistisch sind und viel Quote bringen. Eine Diskussion um die NSA wäre sehr viel sperriger und doch gesellschaftlich sehr viel wichtiger, wie ich finde.«

Frank Schirrmacher fasst das Themenspektrum, mit dem sich Journalisten jetzt befassen sollten, eine Nummer größer: Das eigentliche Thema sei die Frage der Macht. »Wer hat die Macht über die Maschinen?« formuliert er in seiner E-Mail an den »journalist«. Wenn sich das staatliche Gewaltmonopol mit Industriegiganten der Informationsökonomie verbinde, habe ein neues Spiel begonnen, warnt er. »Ein wirklicher Albtraum«, so der Zeitungsmann. Neuland? Man werde sich noch wünschen, dass das Netz für die Politiker Neuland war:

> *»Alle digitalen Texte werden von Maschinen der Überwachung gelesen. Jedes menschliche Verhalten wird in der digitalen Ökologie selber zum Text, der überwacht, gescreent, gewichtet, auseinandergeschraubt wird.*

> *Interpunktion, Grußformeln, Abkürzungen werden zum Distinktionsmerkmal, Fotos werden gescannt und Gedanken rekonstruiert und vorhergesagt, kurz: andere bestimmen jetzt die 'wahre' Rationalität von Texten. Das trifft den Journalismus im Innersten. Das, worüber er Kontrolle zu haben glaubt, seine Sprache wird ihm entwendet. In einer Welt des algorithmischen Doppelagententums, in denen die Netzwerke, denen man sich anvertraut, Spione und potentielle Verräter sind, ändert sich weit mehr als wir uns heute vorstellen können.«*

Die Worte Schirrmachers erinnern stark an die Prophezeiungen eines anderen »Herausgebers«. Ein Herausgeber von Geheimnissen, der seit eineinhalb Jahren in der ecuadorianischen Botschaft in London festsitzt: Julian Assange hatte bereits im vergangenen November in einem Schaltgespräch mit dem Autor das düstere Bild einer Daten-Dystopie an die Wand gemalt: Die millionenfachen Abhörmaßnahmen und die massenhafte Speicherung von Informationen träfen auf immer anspruchsvollere Suchalgorithmen. »Eine massive, beispiellose Transformation von Macht. Denn Information ist Macht.«

Sollten sich Journalisten zusammenschließen, um gegen die ausufernde Überwachung zu protestieren? »Das würde ich gar nicht als Journalist tun«, sagt Georg Mascolo. »Das tue ich als Staatsbürger. Der Journalist ist nach Artikel 5 selbst Grundrechtträger.«

Was aber ist dann die Aufgabe der Medien angesichts dieses Datenschutz-Supergaus? Journalisten müssten jetzt »tit for tat« spielen, fordert Frank Schirrmacher. Sie sollten gegenscreenen, erzählen, durchleuchten, zeigen und übersetzen, was digitale Überwachung heißt. Dazu müsse man nicht undercover in der NSA recherchieren. Es genüge, dort zu beginnen, wo die Maschinen ansetzen: bei der Sprache der gegenwärtigen Politik.

Und Vertrauen zurückgewinnen. Gleich zweimal innerhalb kürzester Zeit sind Informanten nicht direkt zu den großen Medienhäusern gelaufen, sondern haben sich mit ihrem Material lieber an einen bloggenden Journalisten bzw. an eine Organisation wie WikiLeaks gewandt. »Wir müssen uns fragen, ob wir was falsch machen, dass

solche Geschichten nicht unmittelbar bei uns laufen«, sagt Georg Mascolo selbstkritisch und liefert die Antwort gleich hinterher: »Es gab Zeiten, da sind Insider mit ihren Informationen auf direktem Wege zu uns gekommen. Und ich möchte eigentlich auch, dass das so bleibt.«

Immerhin, den beiden Watergate-Reportern, Bob Woodward und Carl Bernstein, war es vergönnt, den Namen ihres Informanten gegen zahlreiche Attacken geheim zu halten – und das stolze 33 Jahre lang. »Erst wenn Deep Throat stirbt, werden wir seine Identität preisgeben, so wie wir es immer versprochen haben«, schreibt Bernstein in »Der Informant«. Ein Versprechen, das heute kein Journalist mehr machen sollte.

Dieser Text ist zuerst am 1. September 2013 in »journalist«, Ausgabe 8/2013 erschienen.

Prism Break – Season 1

Richard Gutjahr

Die Snowden-Saga folgt der klassischen Dramaturgie einer TV-Serie. Woche für Woche neue Enthüllungen mit immer neuen Eskalationsstufen. Für alle, die den Überblick verloren haben, hier der ultimative Episoden-Guide der ersten Staffel.

> *Ein junger Programmierer ohne Schulabschluss stößt auf eine gigantische Regierungsverschwörung. Er fasst sich ein Herz, geht damit an die Öffentlichkeit und wird zur meistgesuchten Person der Welt. Seine Lebensversicherung sind die Daten, die er bei sich trägt und auf die es alle abgesehen haben. Während die beteiligten Regierungen bemüht sind, die Angelegenheit herunterzuspielen, greifen die Machthaber hinter den Kulissen zu immer skrupelloseren Methoden, um den Mann zum Schweigen zu bringen.*

Die Snowden-Saga folgt geradezu lehrbuchmäßig der sog. *Helden-Reise*, wie sie an Drehbuch-Schulen gelehrt wird: Ein Held wider Willen wird in dunkle Machenschaften verstrickt, wird um die halbe Welt gejagt und muss sich einer schier unlösbaren Prüfung stellen, um am Ende, geläutert und gereift, als Sieger hervorzugehen. An seiner Seite eine Gruppe von Gefährten, die mit primitivsten Waffen gegen die finsteren Mächte kämpfen. Seine Nemesis: Das System, in Gestalt des US-Präsidenten und seiner Spooks.

Events Occur in Real Time

Der Aufbau des NSA-Skandals folgt einer klassischen TV-Serien-Dramaturgie. Woche für Woche eine neue haarsträubende Enthüllung. Daraufhin die immer drastischer werdenden Reaktionen der Regierung. Mit jeder Folge zieht sich die Schlinge um den Hals des Helden weiter zu.

Kurz vor Ende der ersten Staffel, nun also der erste große Showdown: Mit der vorübergehenden Festnahme des Lebenspartners eines

Reporters und der Zerstörung zweier Festplatten hat die britische Regierung dem Guardian offen den Krieg erklärt. Ein symbolischer Akt, der Journalisten weltweit dazu zwingt, Stellung zu beziehen.

Episoden-Guide Season 1

Wegen der Urlaubszeit mag vielleicht der eine oder andere von Euch eine Folge verpasst haben. Deshalb hier nun also der ultimative Episoden-Guide von Prism Break – Events occur in Real Time:

S01E01 »Living the American Dream«

Edward Snowden lebt den amerikanischen Traum: Haus auf Hawaii, die Freundin eine Tänzerin. Sein Job beschert dem jungen Paar ein stattliches Auskommen. Niemand ahnt, dass der 29-Jährige einen Entschluss gefasst hat, der nicht nur sein Leben für immer verändern wird. Die Enthüllung des größten Überwachungssystems in der Geschichte der Menschheit.

S01E02 »Red Pill Blue Pill«

Snowden kontaktiert einen Journalisten und weiht ihn in seine Pläne ein. Doch der Reporter verlangt Beweise. In einer komplizierten Prozedur kommt es schließlich zu einem persönlichen Treffen in Hong Kong. Doch die NSA hat bereits Verdacht geschöpft und macht sich auf die Suche nach dem abtrünnigen Programmierer.

S01E03 »Tsunami«

Die Veröffentlichung der ersten Geheimdienst-Papiere – ein diplomatisches Erdbeben rund um den Globus. Die Berichte zwingen den US-Präsidenten, vor die Kamera zu treten, um Schadensbegrenzung zu betreiben. Snowden weiß, dass ihm nur noch wenig Zeit bleibt bis seine Verfolger ihn ausfindig machen. Er sucht Schutz in der Öffentlichkeit, präsentiert ein Video, in dem er sich und seine Motive erklärt.

S01E04 »Escape«

Flucht aus Hong Kong, nachdem Snowden einen Tipp bekommen hatte, dass er hier nicht mehr länger sicher sei. In letzter Minute gelingt es ihm, den Flieger nach Moskau zu besteigen. Die Chinesen lassen ihn ziehen, berufen sich auf die falsche Schreibweise von Snowdens Namen auf dem offiziellen US-Auslieferungsgesuch.

S01E05 »Transit«

5.000 Bonusmeilen später. Die Weiterreise von Moskau nach Südamerika gestaltet sich als schwierig. Snowden besitzt keine gültigen Papiere, Asylgesuche werden der Reihe nach abgelehnt. Kein Land möchte es sich mit den USA verscherzen. Unterdessen weitere peinliche Enthüllungen: Der Britische Geheimdienst hat die Delegationen des G20-Gipfels in London ausspioniert. Die NSA soll Botschaften und EU-Gebäude verwanzt haben.

S01E06 »Neuland«

Der US-Präsident in Berlin zu Gast bei Freunden. Freunde, die er millionenfach bespitzeln lässt, wie den neuesten Snowden-Enthüllungen zu entnehmen ist. Der geplante Jubel-Auftritt am Brandenburger Tor verkommt zum peinlichen Schmierenstück. Obama, Gauck und Merkel ringen nach den richtigen Worten, finden sie aber nicht – der Rest ist Neuland.

S01E07 »I Bolive I Can Fly«

Die US-Regierung erhebt offiziell Anklage. Snowden drohen 30 Jahre Haft. Begründet durch ein Spionage-Gesetz, das aus der Zeit vor dem 1. Weltkrieg stammt. Diplomatischer Zwischenfall in Wien: Die USA zwingen den Bolivianischen Präsidenten zur Notlandung, weil sie an Bord seiner Maschine Edward Snowden vermuten – fälschlicherweise, wie sich später herausstellt. In der Folge bieten Ecuador und Nicaragua Snowden Asyl an.

S01E08 »Least Most Untruthful«

Geheimdienstkoordinator Clapper unter Druck. Er muss einräumen, dass er gelogen hat, als er unter Eid aussagte, er wisse nichts von einer massenhaften Überwachung des amerikanischen Volkes. Es sei die »am wenigsten unwahre« Antwort gewesen. Unmut macht sich breit in Washington. Mit einer dünnen Mehrheit von gerade mal 12 Stimmen wird im Kongress das neue Budget des Spionageprogramms bewilligt. Ein Schuss vor den Bug.

S01E09 »From Russia With Love«

Edward Snowden nimmt das Asylangebot des früheren KGB-Chefs Vladimir Putin an und verlässt den Transitbereich des Moskauer Flughafens. Das Weiße Haus ist außer sich, sagt die Teilnahme an einem Gipfelgespräch mit den Russen ab. Ein Bericht über das Programm XKeyscore versetzt die Deutschen in Aufregung. Der BND räumt ein, das Programm, mit dem sich die Kommunikationsströme von Privatpersonen weltweit in Echtzeit überwachen lassen, zu besitzen – »zu Testzwecken«. Innenminister und Geheimdienstkoordinator erklären die Affäre, die keine ist, für beendet.

S01E10 »Black Helicopters«

Eine weitere Enthüllung erschüttert die USA. Entgegen aller Beteuerungen seien auch US-Staatsbürger tausendfach überwacht worden – ein klarer Verstoß gegen die Verfassung. Angeblich habe man die Vorwahl von Ägypten mit der von Washington D.C. verwechselt, heißt es zur Begründung. Jetzt überschlagen sich die Ereignisse. Der Lebensgefährte des Reporters, der mit seinen Berichten den Skandal ins Rollen brachte, wird am Flughafen vorübergehend festgenommen. Der Chefredakteur des Guardian erklärt, er sei gezwungen worden, die Festplatten zweier Computer im Keller des Redaktionsgebäudes zu zerstören. Der Auftrag dazu sei direkt aus der Downing Street gekommen. Eine Kriegserklärung. Chefredakteur und Reporter erklären, man werde die Berichterstattung nun noch aggressiver fortsetzen.

Dieser Text ist zuerst erschienen auf Richard Gutjahrs Blog[18]*.*

Bürger sucht Staat: Edward Snowden und das nicht-wirtschaftliche Moment der digitalen Gegenwart

Krystian Woznicki

Die Debatten in der Post-Snowden-Welt übersehen meistens einen wichtigen Punkt: Überwachung, das vermeintliche Produkt des Staats, ist ebenso ein Baby der privaten Wirtschaft. Ob Werkzeuge oder Experten, Infrastruktur oder Ideologie – Überwachung wird heute maßgeblich vom Markt geprägt. Edward Snowden stellt sich mit seinen Enthüllungen in mehrfacher Weise gegen diese Entwicklung. Auf diese Weise belebt er die Figur des Bürgers und zieht den Staat zur Verantwortung. Berliner Gazette-Herausgeber Krystian Woznicki kommentiert.

Total-Überwachung gehört in westlichen Demokratien zu den angenommenen und zu den geduldeten Szenarien. Die weit verbreitete Akzeptanz geht auf die Neuzeit zurück. Die staatlichen Überwacher galten als Beschützer – sowohl in der Gestalt von distanzierten Autoritäten als auch von konkreten Vertrauenspersonen im Alltag der Bürger. Sie profilierten sich durch Fürsorge, Verantwortung, Wachsamkeit und boten größtmöglichen Schutz – sowohl für den Einzelnen als auch für dessen Eigentum. Insbesondere nachts, wenn die meisten schlafen. Für dieses Rundumversorgungspaket erwarteten die Überwacher Disziplin und Gehorsam. Man musste sich an deren Normen und Gesetze halten.

Das waren in der Neuzeit »Stoff, Form und Gewalt eines staatlichen Gemeinwesens« (Thomas Hobbes). Und heute? Der Staat bietet nicht mehr Schutz, sondern Sicherheit. Das ist ein entscheidender Unterschied. Neuerdings zum »Super-Grundrecht« (Hans-Peter Friedrich) avanciert, dient Sicherheit als Legitimation für verfassungswidrige Operationen. Für den Staat ist in Friedenszeiten jeder Exzess denkbar: Ob nun für die paranoide Übererfüllung seiner Beschützerfunktion oder für die Vernachlässigung eben dieser Pflicht.

Die seit dem 11.09.2001 unablässig »boomende Sicherheitsindustrie« (Naomi Klein) katalysiert beide Extreme: Der mit der privaten Wirtschaft verwachsene Überwachungsstaat ist den Produktversprechen der Sicherheitsfirmen erlegen und wird im Zuge dessen zu neuartigem Größenwahn beflügelt. Andererseits entzieht er sich seiner Verantwortung, wenn er Überwachung an private Dienstleister auslagert.

Duldung und Division

Der Fall Snowden zeigt: Die Zumutungen haben einen Punkt erreicht, an dem die Duldung einem Aufbegehren weicht. Aus »ich weiß, dass ich Zugang zu ungeheurem Wissen habe« wird »ich kann nicht länger mit dem Wissen um dieses Wissen leben«. Snowdens innere Kehrtwende wäre ein Identifikationsangebot unter vielen, wenn das Problem nicht uns alle beträfe. Und so drängt es sich geradezu auf, dass zudem aus »wir wissen, dass wir nicht wirklich wissen wollen, wie es nun genau ist« so etwas wird wie »wir können nicht länger mit dem Wissen um unser Nicht-Wissen-Wollen leben«.

Darüber hinaus zeigen Snowdens Enthüllungen über die Zusammenarbeit zwischen Staaten und transnationalen IT-Konzernen: Die Überwacher sind auf maximale Distanz zu ihren Subjekten gegangen, die sie nur noch datentechnisch erfassen, einsortieren und analysieren wollen, aber für die sie nicht mehr sorgen wollen, geschweige denn Verantwortung übernehmen wollen.

Eine tiefe Kluft tritt deutlicher denn je zu Tage: Die Division zwischen Staat und Bürger. Das zeigt sich in den Enthüllungen selbst – sowohl in der großen Erzählung als auch in jedem einzelnen Detail. Und die Berichterstattung über die Enthüllungen zementiert diese Spaltung. Man setzt entweder auf Personengeschichten oder auf die Skandalisierung von Machtmißbrauch. So werden Snowdens Situation und die Inhalte seiner Enthüllungen voneinander getrennt. Kein Bericht strebt eine Synthese an.

Bürger und Staat zusammendenken

Bürger- und Staatsfragen zusammenzudenken, liegt offenbar nicht im Interesse von Journalisten. Selbst jene, die politisch engagiert das Wort ergreifen, verweigern sich in dieser Sache. John Naughton etwa betont, nicht Snowden sei die Geschichte, sondern das, was seine Enthüllungen über die Zukunft des Internet aufzeigen. Lorenz Matzat gibt wiederum zu verstehen, er habe den Staat in dieser Sache abgeschrieben, der Bürger hingegen müsse sich neu sammeln. Jedoch erinnert uns der zwischenzeitig an einem Flughafen gestrandete und dann in Russland Asyl suchende Edward Snowden daran: Ein Staat ohne Bürger und umgekehrt ein Bürger ohne Staat sind nicht denkbar.

Snowden macht deutlich: Wer einen Bürger, der wie Edward Snowden außerordentliche Zivilcourage beweist, zum Staatsfeind erklärt, schwächt nicht nur die Identität des Bürgers. Sondern auch des Staats. Welche Legitimation hat die USA noch als Rechtsstaat, wenn sie berechtigte Kritik aus den Reihen ihrer Bürger unterdrückt? Diese Frage stellt sich insbesondere dann, wenn der Gegenstand der Kritik staatliche Programme sind, die nicht nur auf der Beschneidung von Bürgerrechten basieren, sondern darüber hinaus sogar darauf ausgerichtet sind, Bürger in ihren Freiheiten und Rechten massiv einzuschränken. Wäre dem nicht so, könnten wir folgende Fragen beantworten: Wird Snowden jemals wieder ein freier Bürger sein können? Wird er jemals Anerkennung finden von jenem Staat, dem sein konstruktives Aufbegehren als Bürger gilt? Doch das steht wohl genauso in den Sternen wie der Verbleib des Bürger-Modells an sich.

Die Veränderungen von Staatlichkeit lassen offen, ob und wie wir in Zukunft in der Lage sein werden, uns als Bürger zu begreifen. Welche Rechte werden wir haben? Auf welchen Gesetzen werden sie fußen? Welches Selbst-Bewusstsein wird uns antreiben? Wie groß und in welcher Weise ausgeprägt wird unser Wille zum Politischen sein? Welches Verhältnis zum Staat werden wir haben? Eines ist klar und auch daran erinnert: Sowohl der Bürger als auch der Staat – beides muss immer und immer wieder erkämpft werden, weil beides nicht gegeben ist (allenfalls nur auf dem Papier oder als Lippenbekenntnis). Und weil beides überformt ist durch die Logik des Marktes. Das heißt aber auch,

dass der Kampf sowohl auf der politischen Ebene als auch auf der intellektuellen Ebene geführt werden muss. Wir müssen Staat und Bürger auch neu denken.

Hindernisse und Hürden

Die Kluft zwischen Bürger und Staat ist inzwischen eine immer größere und undurchdringlicher werdende Schattenzone, in der auch PRISM, Tempora und XKeyscore entstehen konnten. Diese Schattenzone rund um die Geheimdienste wird strukturell zusehends ununterscheidbarer von der Schattenzone des Staats, die aufgrund der immer weniger parlamentarischen/demokratischen Prozessen unterworfenen Gestaltung von Politik entsteht. Diese Entwicklung hin zu einem »neoliberalen Staat« (David Harvey) begünstigt die Wirtschaft und ermöglicht die so genannte Private-Public-Partnership sowie die Privatisierung staatlicher Leistungen.

Denn auch so lässt sich die Auflösung des Staats lesen: Er löst sich nicht in Luft auf, stattdessen lösen sich seine vertrauten Konturen und Strukturen auf, an deren Stelle neue treten: Staatliche Überwachungsinfrastrukturen etwa, die in weitgehend undurchsichtiger Weise auf verschiedenen Ebenen privatisiert sind. Erstens werden sie nicht mehr allein von Behörden, sondern zu großen Teilen von privaten Security-Anbietern betrieben. Zweitens kauft der Staat auf dem freien Markt Sicherheitsprodukte ein. Drittens unterstützt der Staat die IT-Industrie mit Subventionen sowie Sonderrechten und bittet im Gegenzug um freien Zugang zu Kundendaten.

Ob die besagten Schattenzonen lediglich eine Begleiterscheinung des Transformationsprozesses sind oder ob sie das Wesen des neuen Staats ausmachen – das wird auch die zivilgesellschaftliche Transparenzbewegung so schnell nicht beantworten können. Zwar adressiert sie mit ihrer Forderung nach Abschaffung der Schattenzonen den richtigen Punkt. Doch zeigt sich schon heute: Nicht nur die Verweigerung der Transparenz, sondern auch das Transparenz-Washing ist ein großes Problem. Apropos: »US-Regierung will Details zur

Telefonüberwachung offenlegen« (Spiegel Online). Das »Offenlegen« wird von hochbezahlten Image-Agenturen betreut. Es zielt auf die Orchestrierung von Transparenz und damit auf die systematische Irreführung jeglichen Engagements seitens der Bürger.

Was bringt der »Snowden-Effekt« in Bewegung?

Ohnehin ist dieses Engagement heutzutage nicht mit allzu rosigen Aussichten aufgeladen. Verglichen mit der Weltrevolution 1968 gehen heute weltweit deutlich mehr Menschen auf die Straße. Die Regierungen sind jedoch weniger denn je gewillt einzulenken, geschweige denn auf die Proteste zu hören. Entsprechend realistisch gibt sich Snowden. Gefragt nach der schlimmsten Konsequenz seiner Enthüllungen über die Überwachungsprogramme sagt Snowden; »dass sich nichts ändert.«

Bereits jetzt absehbar ist, dass der »Snowden-Effekt« (Jay Rosen) einiges in Bewegung bringt. Er setzt unbequeme Themen auf die Agenda von Politik und Massenmedien und hält sie dort erstaunlich lange 'oben'. Nebenbei könnte der »Snowden-Effekt« Bürger und Staat zu einer Renaissance verhelfen und damit Begriffe neu beleben, denen der Beigeschmack einer kafkaesk-verwalteten Welt anhaftet.

Die Frage der Stunde ist, ob und wie Bürger und Staat neu aufgeladen werden können: Kann einer wie Edward Snowden, der sich weitaus seriöser präsentiert als der geistesverwandte Bradley Manning – kann ein solcher Bürger- und Staats-Idealist das Ideal des Bürgers und das Ideal des Staats neu beleben? Und damit gleichsam neue Ideale des Bürgers sowie des Staats definieren helfen?

Von EZLN über WikiLeaks zu Snowden

Edward Snowden hat mehrfach zu verstehen gegeben, dass er mit seinen Enthüllungen der USA nicht schaden möchte – im Gegenteil. Der ehemalige Geheimdienstmitarbeiter entpuppt sich als demokratietheoretisch geschulter Bürgerrechtler, wenn er in seinen Ausführungen auf die Notwendigkeit einer öffentlichen Debatte verweist. Er macht den Schritt an die Öffentlichkeit in einem besonderen Moment: Noch während Bradley Manning der Prozess

gemacht worden ist, sichtlich darum bemüht alle potenziellen Whistleblower einzuschüchtern, legte er Informationen nach, die die von Manning angestoßenen Debatten über das Verhältnis von Staat und Bürger in neuer Weise befeuern.

Während Manning den Rohstoff (Informationen) lieferte, verstand es WikiLeaks den Informationen eine Perspektive, eine Stoßrichtung zu geben: die Rechenschaftspflicht öffentlicher Institutionen reaktivieren. Die Whistleblower-Plattform konnte die an sie gerichteten Erwartungen nicht vollends erfüllen. Doch hat sie ein wichtiges historisches Bindeglied geschaffen zwischen disparaten Ansätzen und Bewegungen, die die Rolle des (aufbegehrenden) Bürgers und die Aufgaben des Staats auf ihre Agenda gesetzt haben. Der Fall Snowden erscheint vor diesem Hintergrund als Speerspitze einer diffusen Bewegung, die so unterschiedliche Strategien verfolgt wie Raumbesetzungen und Online-Aktivismus. Und das in so unterschiedlichen Ländern wie Deutschland und Mexiko.

Einmal aus der Vogelperspektive betrachtet: Die jüngsten Aufstände rund um den arabischen Frühling, die Occupy-Bewegung, netzpolitische Initiativen (u.a. Ad-ACTA) sowie die Riots von Paris bis London beerben die globalisierungskritischen Bewegungen nach den Ausschreitungen von Seattle im Jahre 1999. Ihren Vorläufer haben jene wiederum in den Aktionen der EZLN. Sie besetzen seit den frühen 1990er Jahren eine verarmte Region in Süd-Mexiko und verzichten dabei auf Waffengewalt. Ihren öffentlichen Druck entfalten sie stattdessen medial. Dabei gilt das Aufbegehren nicht primär den multinationalen Konzernen und der globalen Wirtschaft, die als primäre Ursachen für das Elend gelten. Vielmehr wendet sich ihr Widerstand gegen den Staat. Wer sonst könnte Rechte garantieren? Wer sonst könnte den Ausverkauf des Landes und somit auch die Macht der multinationalen Konzerne eindämmen?

Willkommen im Bürgerkrieg!

Es ist eine Bewegung, die sich (noch) nicht als solche begreift. Ob wir hier über die 99% sprechen oder eher eine Minderheit der Weltbevölkerung sei dahingestellt. So oder so: All jene, die sich heute

noch in einem sich auflösenden beziehungsweise im Entstehen begriffenen Rechtsrahmen bewegen und engagieren sind noch »informelle politische Subjekte« (Saskia Sassen), die im bevorstehenden Geschichtsabschnitt zu »formal politischen Subjekten« reifen, sprich; die neuen Bürger werden.

Dass dieser Prozess nicht ohne Kampf möglich ist, daran erinnern Tiqqun. Das Autorenkollektiv aus Frankreich meint: Recht zu haben reiche nicht aus, man müsse auch in der Lage sein, Veränderungen herbeizuführen. Tiqqun ist nicht so dumm Gesetze (und Rechte) für »nutzlos« (Evgeny Morozov) zu erklären, sondern relativiert ihre gesellschaftspolitische Funktion und verweist nicht zuletzt auf das Dilemma der Rechtsdurchsetzung – deren schleichende Privatisierung einerseits, deren Aufhebung andererseits. Konsequenterweise ruft Tiqqun den Bürgerkrieg aus. Unter anderem mit dem Ziel, den Rechtsstaat zu reanimieren.

Man kann den »Snowden-Effekt« mit »Paranoia« und »Getöse« (Otto Schily) abtun, aber damit weder das »Ende der Debatte« (Frank Schirrmacher) legitimieren, noch den »kommenden Bürgerkrieg« in Abrede stellen. Zu ernsthaft bedrohen sowohl die Überwachungsverfahren als auch deren Undurchsichtigkeit die Gesellschaft. Die Vermählung von Staat und Wirtschaft ermöglicht ein post-panoptisches Schattenregime der »sozialen Klassifizierung« (David Lyon), der »kumulativen Benachteiligung« (Oscar Gandy), der »datenbasierten Diskriminierung« (Kurz/Rieger) sowie der »Adiaphorisierung« (Zygmunt Baumann) – derweil sich die Spaltung zwischen Bürger und Staat verschärft.

Bedrohungen, Gegenmittel, Forderungen

Wenn Rechtsstaat und Bürgerschaft erkämpft werden müssen, dann sind Grundrechte nicht alles, aber wichtig. Schutzrechte müssen zugunsten des »Super-Grundrechts Sicherheit« (Hans-Peter Friedrich) verteidigt werden. Datenschutz etwa gehört in der Post-Snowden-Welt ganz oben auf die Agenda. Ebenso die Forderung nach einem

Whistleblower-Schutz. Vielleicht muss sogar eine »Whistleblower-Gewerkschaft« (Ulrich Beck) her.

Die Rechenschaftspflicht öffentlicher Institutionen muss durchgesetzt werden. Geheimdienste sind davon nicht ausgeschlossen. Die Komplexität der Technik, nationale Sicherheit oder Betriebsgeheimnisse privatwirtschaftlicher Partner können nicht ernsthaft als Argumente herhalten um die Undurchsichtigkeit der neuen Überwachungsverfahren zu legitimieren.

Transparenz als Kontrollmechanismus kann ein probates Gegenmittel sein. Doch kann es nicht Transparenz um der Transparenz willen sein. Wir, die Bürger von morgen, müssen uns fragen: Wie wollen wir Transparenz herstellen? Wozu genau? Was dann machen damit? Unreflektierte Transparenz kann nicht zuletzt dem Daten- und Informationsfetischismus zum Opfer fallen. Deshalb gilt auch analog dazu: Leaks nicht der Leaks willen. Es geht vielmehr darum, auf der wachsenden Informationsbasis der Leaks und den daraus resultierenden gesellschaftspolitischen Konsequenzen möglichst bald nicht nur noch mehr Informationen zu leaken, sondern auch Medizin, Essen, Häuser und öffentliche Netz-Infrastrukturen.

Das nicht-wirtschaftliche Moment

Zu Beginn des 21. Jahrunderts lösen Konzerne aus dem IT-Bereich das Militär als Technologie-Avantgarde ab. Darüber hinaus ersetzen sie den Staat als Container, in dem wir uns aufgehoben fühlen. Die Allgegenwart der Ökonomisierung zeitigt nicht nur einen neoliberalen Staat, sondern auch Sinnsysteme wie Facebook, die Menschen das ersehnte Gefühl von Zugehörigkeit vermitteln. Hier ist das Verhältnis von Bürger und Staat an einem Nullpunkt angekommen. Hier ist es in fortgeschrittener Auflösung begriffen.

Wollen wir das Verhältnis von Bürger und Staat neu im Konnex Technologie und Zugehörigkeit denken – dann gilt es nicht zuletzt für das »nicht-wirtschaftliche Moment« (Philippe Aigrain) unserer digitalen Ära zu sensibilisieren. Wie auch immer das Selbstverständnis als

Mitglied eines sozialen Netzwerks (ob Kunde, Konsument oder Produkt, ob unfreiwillig oder selbstbestimmt überwachtes Objekt), längst überformt es das Mindset des Bürgers. Sich als Bürger neu zu begreifen (mit allem was dazugehört, mit allen Konsequenzen, auch im Hinblick auf den Staat) das bedeutet heute, das »nicht-wirtschaftliche Moment« auf die eigene Existenz zu beziehen. Sich als Bürger zu rekonzipieren bedeutet Nicht-Kunde, Nicht-Konsument, Nicht-Produkt der (Selbst-)Überwachung zu sein. Zumindest für einen Moment, in dem sich potenziell alles neu ordnet.

Schließlich bedeutet es Bürgerschaft mit anderen zu teilen – als Lebensgefühl, als Gesinnung, als innere Notwendigkeit. Wie es Edward Snowden mit uns tut: Statt weiterhin ein Angestelltendasein zu fristen, hat er sich, seinem Gewissen folgend, auf seine Rolle als verantwortungsvoller Bürger besonnen. Statt die Informationen an den Meistbietenden zu verkaufen, macht er sie der Öffentlichkeit in Zusammenarbeit mit glaubwürdigen Journalisten frei zugänglich. Statt sich von den Massenmedien als Widerstandspopstar feiern zu lassen, lässt er sein Wissen sprechen. Zwecks konstruktiver Kritik am Staat. Snowden zeigt damit nicht zuletzt, dass das »nicht-wirtschaftliche Moment« ein besonders kostbares Moment ist in Zeiten, die hoffnungslos überladen scheinen mit den Werten und der Logik des Marktes. Darüber hinaus zu denken, fällt schwer. Etwa genauso schwer, wie sich selbst als Bürger und den Staat als Rahmen der eigenen Existenz zu begreifen. Wie das doch möglich ist – das führt Snowden in einer sehr radikalen Weise vor.

Dieser Artikel ist zuerst am 20. August 2013 in der Berliner Gazette erschienen [19]

Es ist keine Spähaffäre

Torsten Kleinz

Am Wochenende sah ich an einem Kiosk die Schlagzeile der »Welt«: Online-Banking im Visier der Geheimdienste«. Und ich stoppte für zwei Sekunden und dachte nur: *NEIN. Das ist eben nicht die Neuigkeit. Wisst ihr denn gar nichts???* Und dann sah ich darunter die Überschrift:"So erleben Sie die interaktive Zeitung«. Und ich dachte mir nur: Ja. Ihr wisst nichts.

Um es klar zu sagen: Online-Banking ist nicht im Visier der Geheimdienste. Sie scheren sich einen Dreck darum, wann Ihr die GEZ-Gebühren überweist, wie viel Nebenkosten ihr für Eure Wohnung überweisen müsst und ob Euer Dispo 700 Euro oder 1200 Euro ist. Es sei denn ... Es sei denn, es ergibt sich ein Muster. Es ist der Zauber von Big Data, dass quasi alles ein Muster ergeben kann.

Die öffentliche Wahrnehmung kann noch nicht wirklich damit umgehen. Die seriöseren Medien haben den NSA-Skandal zur »Spähaffäre« gemacht. Das klingt sachlich, ein wenig abstrakt, nicht allzu anklagend und ergibt eigentlich überhaupt keinen Sinn. Denn wer späht denn da was aus? Das Bild stimmt einfach nicht mehr. Es gibt keinen Techniker, der in einem Hauptquartier mit großen Kopfhörern sitzt und gezielt unsere Gespräche mitschneidet, keine Geheimagenten, die uns in verfänglichen Situationen fotografieren. Das heißt: Diese Leute gibt es zwar noch, aber sie sind nicht Teil des NSA-Skandals.

Korrekter wäre wohl »Speicherskandal«. Denn das ist es, was NSA und ihre Partner in vielen anderen Ländern machen: Sie entreißen die Kommunikation von Milliarden Menschen ihrer Umgebung und speichern sie in gewaltigen Rechenzentren ab. Und weil selbst die gewaltigsten Kapazitäten und Geheimbudgets nicht ausreichen, wirklich alles zu speichern, suchen die Geheimdienstanalysten nach Mustern, um zu entscheiden, was mehr als ein paar Tage auf den Datenspeichern bleiben soll.

Doch »Speicherskandal« klingt langweilig. Denn unsere gesamte Kommunikation besteht daraus, dass Daten gespeichert, kopiert und weitergesandt werden. Die NSA oder die GCHQ oder irgendwer anders setzt einen Speichervorgang hinzu und liest diese Informationen wahrscheinlich nicht einmal. Wo ist das ein Skandal, wenn man das mit Facebook vergleicht, mit dem Datenhunger von Google, Apple, Amazon, die uns tatsächlich überzeugten, es wäre viel besser, wenn wir unsere Daten nur noch leihweise kontrollierten? Haben wir wirklich erwartet, dass Geheimdienste still im Kämmerlein sitzen und das Internet an sich vorbeiziehen lassen? *Das nennt ihr einen Skandal? Get real!*

Doch: Es ist ein Skandal, und zwar kein kleiner. Denn die allumfassende Speicherung von Daten, die ihren Kontexten entrissen wurden, ist nicht nur ein Vertrauensbruch. Die Geheimdienstler, die unsere Techniken systematisch schwächten, haben auch an den Grundfesten gerüttelt, auf denen das Internet aufgebaut wurde. *Große Worte, aber was heißt das?*

Nun: Die vielen stückweisen Enthüllungen von Edward Snowden geben uns einen Vorgeschmack. Denn Snowden macht dies ohne erkennbares Gewinnstreben und hat sein bisheriges Leben weggeworfen. Wie viele andere NSA-Leiharbeiter da draußen gibt es, die vermeintlich schlauer waren und diese Informationen weiterverkauft haben? Oder die nicht schlauer waren, sondern selbst abgelauscht wurden? Wie viele Millionen Informatiker kann China drauf ansetzen, die Schwachstellen zu finden, die die NSA offen gelassen hat? Digitale Horchposten sind keine Einbahnstraße. Was Richtung Utah geschickt wird, landet vielleicht auch in Peking. Dass die USA chinesischen Hardwareunternehmen unterstellen, Spionagekomponenten einzubauen – soweit ich weiß ohne bisher Beweise geliefert zu haben – lässt erahnen: Was machen die US-Hardwareunternehmen? Doch was hat das mit uns zu tun? Als Politiker, der Freihandelsabkommen oder Militärschläge beraten muss, würde ich kein Outlook einsetzen wollen, kein GMail, kein Windows. Ich würde übrigens auch nicht auf eine Yandex-Alternative setzen oder das Rote-Fahne-Linux einsetzen. Und der Normalbürger?

Ja, der Normalbürger kann sich in der »Ich habe nichts zu verbergen«-Illusion sonnen. Denn den NSA interssiert nicht wirklich, mit wem Max

Mustermann Geschlechtsverkehr hat, welche Medikamente er nimmt, ob er hinterrücks falsche E-Mails verschickt um einen Kollegen anzukreiden. Die Geheimdienste durchwühlen Eure Daten und lassen meist keine Spuren zurück. Meist. Bisher.

Eine der beunruhigendsten Enthüllungen der letzten Zeit stammt von vergangener Woche und sie hat für wenig Aufsehen gesorgt: Demnach wurden nicht nur Milliarden Telefondaten an die Geheimdienste weitergegeben, sondern auch eine spezialisierte Einheit aufgebaut, die den Beweisprozess verfälschte. Kurz gesagt: Die Geheimdienste sollen in ihrer gewaltigen extra-legalen Datenbank Spuren gesucht haben und dann anderen Strafverfolgern den Tipp gegeben haben, welche legalen Daten denn zu einem Erfolg führen konnten. Vor Gericht landeten dann eben nur die offiziellen Polizei-Erhebungen. Wie sie denn darauf kamen, Anschluss XYZ abzuhören oder das Hotmail-Konto von Zeugen ABC ausliefern zu lassen – wer weiß das schon? Solide Polizeiarbeit halt. *Und dennoch – warum sollte das den Normalbürger interessieren, der nichts verbrochen hat?*

Weil es ihn auch treffen kann. Mit einer zunehmenden Wahrscheinlichkeit. Denn jeder muss sich nur die rechte Spalte auf Facebook ansehen, um zu erkennen, wie fehlerhaft Big Data doch ist. Die Technik hinter Facebook-Anzeigen ist im Prinzip nicht viel anders als das, was Geheimdienstanalysten machen: Sie suchen Muster in Deinen Postings und denen Deiner Friends und versuchen, daraus Schlüsse zu ziehen. Dazu kommen noch allerhand Mutmaßungen, IP-Daten und ein Schuss Werbe-Voodoo. Dass sie damit in 999 von 1000 Fällen falsch liegen müssen ist ja egal. Bei Facebook macht die Masse der Klicks das Versagen weniger relevant, bei den Geheimdiensten wird die Erfolgskontrolle systematisch verhindert. Und das nicht nur, weil erfolgreiche Geheimdienstarbeit spektakuläre Anschläge verhindern mag, sondern weil die Kontrollgremien irrelevant gemacht wurden. Und die interne Kontrolle der NSA so motiviert ist wie die Doping-Kontrolle zu Zeiten von Lance Armstrongs großen Tour-Erfolgen.

Das Teuflische an Big Data ist auch: Es wird Dich niemals entlasten. Die Verdachtsmuster summieren sich von Mal zu Mal und niemand kann Dir

sagen, was denn zu einem Rabatt führt. Du hast 80 Mal das Flugzeug benutzt ohne dass Du aufgefallen bist? Mach Dich nicht lächerlich: Auf der No-Fly-Liste gibt es keinen Rabatt. Und wir haben immer mehr solcher Listen.

Mir gehen die Metaphern aus. Es ist als ob jedes millionste Auto auf Kommando explodiert? Nein, es explodiert nicht, Du Idiot. Du musst bei jedem dritten Flug zwei Stunden mehr warten. Dein Gepäck wird durchsucht. Deine Telefonrechnung, von der Dich nur der Endbetrag interessiert, landet für einen Sekundenbruchteil im Arbeitsspeicher eines Analysten, der rauszukriegen versucht, wer Geld nach Syrien überweist. Oder ob ihn sein Freund betrügt – wer weiß das schon?

Dieser Artikel ist zuerst am 11. September 2013 auf netzpolitik.org erschienen [20]
.

»Geheimdienste abschalten«

Warum Widerstand es enorm schwer hat

Lorenz Matzat

Das fundamentale Problem des Widerstands gegen die Internetüberwachung ist deren Ungreifbarkeit. Weite Teile der Bevölkerung haben wenig bis keine Ahnung, wie das Internet funktioniert. Es interessiert sie in der Regel auch nicht – Hauptsache es funktioniert. Zum Kommunizieren und Informieren, zum Shoppen und Inhalte konsumieren. Das prophylaktische Ausspähen des Internetverkehrs beeinträchtigt ihren Netzalltag nicht.

Die Binnenansicht der netzpolitischen sowie bürgerrechtlich Engagierten und Interessierten auf NSA, PRISM, Tempora & Co ist eine andere: Hier herrscht Empörung und Erschrecken über die Erosion von Bürgerrechten, vom Ende der Privatsphäre. Hier gibt es zwei Lager; das eine der Staatsgläubigen, die das Ganze für eine Fehlentwicklung halten und denken durch bessere demokratische Regeln wären Geheimdienste in den Griff zu bekommen. Das andere Lager bilden diejenigen, die staatsskeptisch sind und den Fehler im System sehen: Geheimdienste ließen sich per se nicht kontrollieren, seien grundsätzlich undemokratisch. Diese unterschiedlichen Sichten werden ein Problem für eine Bewegung gegen die Überwachungsprogramme darstellen, weil sie auf verschiedene Strategien hinauslaufen: reformistische oder radikale. Ob hier gemeinsame Ziele überhaupt möglich sind, muss sich noch zeigen.

Der Wirtschaftsfaktor

Neben der Problematik der »Bewegung«, das Thema zu vermitteln und sich auf Ziele zu einigen, wird die Debatte oft nicht in einen wirtschaftlichen Zusammenhang gestellt. Die Überwachungsindustrie hat einen enormen ökonomischen Faktor. Wenn alleine in den USA schon über 50.000 Millionen Dollar[21] im Jahr aus schwarzen Kassen von

den verschiedenen Geheimdiensten ausgegeben werden können, hängen mehrere 100.000 Jobs sowie einiges an »Sharehoder Value« von diesen Geldern ab. Die Überwachungsindustrie ist Teil der Rüstungsindustrie und deren Unternehmen haben kein Interesse am Ende der Überwachung[22]. Eine Protestbewegung würde das Geschäftsmodell in Frage stellen und dürfte bekämpft werden. Die Interessen der Staatsangestellten, die in diesem Bereich arbeiten, spielen eine weitere Rolle: In der Regel haben Institutionen bzw. ihre Mitarbeiter einen ausgeprägten Selbsterhaltungstrieb und neigen zum Aufblähen. Stellen und Budgets werden mit Zähnen und Klauen verteidigt.

Zudem scheinen die Überwachungsprogramme der Industriespionage und Wirtschaftsinformation zu dienen; dieses Motiv ist wahrscheinlich ein wesentlicher Faktor; nicht zuletzt weil prosperierende heimische Unternehmen auch wieder durch Steuereinnahmen Geld in die Staatskassen spülen. Aus »betriebswirtschaftlichen« Gründen macht es selbstverständlich Sinn, die Möglichkeiten der teuren Überwachungsinfrastruktur wenigstens zweitzuverwerten. Übrigens wäre es äußerst interessant, zu erfahren durch welche Mechanismen Erkenntnisse der Wirtschafsspionage an Politik, Branchenverbände und Unternehmen fließen: Geschieht dies durch informelle Mitarbeiter, Briefings oder nicht-öffentliche Tagungen?

Die Terrorrhetorik[23], die eine Existenz großer Terrornetzwerke beschwört, scheint vornehmlich ein Narrativ zu sein, mit dem nach innen und außen die enormen Kosten für die Sicherheitsstrukturen gerechtfertigt werden. Wofür braucht der Bundesnachrichtendienst BND neben Pullach den Monsterneubau in Berlin mit Büroflächen, die 35 Fußballfeldern entsprechen und 4.000 Arbeitsplätze beherberge[24]?

Internationales

Ein weiteres Problem im Umgang mit den Überwachungsprogrammen: Vorangetrieben werden sie von den USA, im Bündnis oder in Kooperation mit Regierung oder zumindest den Geheimdiensten zahlreicher Staaten. Kritik an den USA wird schnell des »Anti-

Amerikanismus« bezichtigt; zum Teil berechtigterweise, weil mit Vorurteilen und verquasteten Ideologieversatzstücken oder Antisemitismus hantiert wird. Andererseits ist der Vorwurf des »Anti-Amerikanismus« ein wohlfeiles Totschlagargument, das sich der kritischen Auseinandersetzung mit den nicht selten rücksichtslosen US-Interessen verweigert.

Klar ist jedenfalls, dass es beim globalen Überwachungsprogramm nur mehr Kontrolle oder ihre Abschaltung nur zusammen mit den USA gibt. Dass die Militärdemokratie USA Überprüfungen – etwa durch UN-Strukturen – der Datenfarmen ihrer Geheimdienste zustimmen wird, ist wenig wahrscheinlich. Ganz abgesehen davon, dass die USA notorisch die Unterzeichnung oder gar Ratifizierung diverser internationaler Vereinbarungen verweigert. Was wird sich von Zusagen oder Versprechen von Geheimdienste bzw. ihren Regierungen halten lassen, sich an Regeln und Datenschutzvorgaben zu halten, ohne dass es ein internationales, unabhängiges Kontrollsystem gibt?

Widerstand

Wie könnte konkreter Widerstand gegen die Überwachung aussehen? Sitzblockaden vor Geheimdiensteinrichtungen werden nicht viel erreichen, weil sie die Arbeit dort nicht wirklich behindern. Entgegen der Anti-AKW-Bewegung, der es gelang, nicht nur den politischen Preis in die Höhe zu treiben. Sondern auch den tatsächlichen Preis für Atomkraft, zum Beispiel durch jahrzehntelangen Protest gegen die »Entsorgung« von Atommüll in Gorleben. Der Widerstand gegen Atomkraft war aus zwei Gründen erfolgreich: Niemand stellte in Frage, dass Atomkraft gefährlich ist. Hiroshima und Nagasaki, Tschernobyl und Fukushima waren unleugbar geschehen.

Zum Zweiten hat sich der Widerstand gegen den Bau von Atomanlagen in Deutschland nie entlang der Militanzfrage spalten lassen. Diese Frage ist eine komplizierte; stellt sie doch das Gewaltmonopol des Staates in Frage und sorgt so gleichzeitig für einen medialen Aufmerksamkeitsschub. Der handfeste Charakter des Widerstandes, der von Autonomen und Bauern zusammen oder zumindest geduldet

nebeneinander im Wendland praktisch wurde, machte einen bedeutenden Teil seiner Ausstrahlung aus. Der gemeinsame Konsens war: Gewalt gegen Sachen wurde als legitim erachtet.

Die netzpolitische Bewegung hierzulande ist weit davon entfernt, überhaupt eine Militanzdebatte führen zu müssen. Nicht zuletzt, weil sie bei Weitem keine Bewegung ist: Sie wird weder von unterschiedlichen Bevölkerungsgruppen getragen, noch ist sie zahlenmäßig beeindruckend, noch hat sie bislang Ausdauer bei Protestformen gezeigt. Wenn überhaupt könnte man das Anonymous-Kollektiv und andere Hackerkreise als »militanten« Arm der »Bewegung« verstehen. Doch die scheinbare Stärke im Netz, Effekt der Selbstreferenz (»filter bubble«), hat mit der tatsächlichen gesellschaftlichen Relevanz wenig gemein. Das vorläufige Scheitern der hiesigen Piratenpartei – wenn man so will, der parlamentarische Arm der Netzbewegung – bestätigt dies.

Ohne eine Rückkopplung in die physische Welt, in der Dinge nicht verlustfrei kopierbar sind, wird eine Netzbewegung kaum Wirkung entfalten können. Zudem ist neben dem eingangs erwähnten Vermittlungsproblem keine ausufernde, sondern nur eine punktuelle Repression zu beobachten. Die Bedrohungszenarien, die aufgrund der Internetüberwachung denkbar sind, betreffen bislang nur sehr wenige – für die meisten bleibt sie eine virtuelle Bedrohung.

Perspektiven

»Geheimdienste abschalten« und Vergesellschaftung der bisher gesammelten Daten[25] – dies könnten Forderungen einer Protestbewegung sein. Angesichts des internationalen Charakters des Internets müssten diese global sein. Die Chancen darauf stehen schlecht, weil es trotz der grenzübergreifenden Kommunikationsinfrastruktur Internet äußerst schwer ist, eine globale Protestbewegung zu bilden. Das Aufflammen und der Niedergang von »Occupy« hat das gezeigt. Es fehlt letztlich ein gemeinsames und konkretes Ziel sowie vor allem Ausdauer.

Überhaupt bräuchte es eine Verständigung darüber, wie die Internetüberwachung zu bewerten ist. Sie wird längst nicht von allen als

Ausdruck eines politisch-wirtschaftlichen Systems, als Machtinstrument gesehen. Sondern nicht selten als isoliertes Datenschutz- und Bürgerrechtsproblem verstanden. Ein Sammelbecken, ein Diskursraum, um sich darüber auseinanderzusetzen und sich zu koordinieren, fehlt. Dabei gibt es Vorbilder für solche internationalen Strukturen: Z.B. die Weltsozialforen oder die intergalaktischen Treffen in den Neunzigern in Folge des Aufstandes der Zapatisten im mexikanischen Chiapas. Jedenfalls kann es nicht die alleinige Strategie sein, NGOs nach Brüssel, zum Weltwirtschaftsforum in Davos oder zu UN-Konferenzen zu schicken, damit sie dort an den Rockzipfeln der Mächtigen zupfen.

Insofern lässt sich leider nur ein ernüchterndes Fazit ziehen: Mehr als Verteidigung ist derzeit nicht drin. Sprich, sich auf das Wettrüsten gegen die Sicherheitsapparate einzulassen; also zu versuchen, sichere Kommunikations- und Infrastrukturen zu bewahren und auszubauen. Vielleicht gelingt es auf internationaler Ebene, die von den USA dominierte Kontrolle der Internetinfrastruktur zu mindern. Hoffnung auf Parteien oder gar die neue Bundesregierung braucht man wohl nicht zu setzen. Solange sich keine außerparlamentarische gesellschaftliche Kraft bildet, die viele überzeugt mit Ausdauer eine andere Gesellschaft anzustreben, werden wir weiter überwacht werden.

Der Kampf gegen Korruption und der Schutz von Whistleblowern

Dr.Christian Humborg

Seit nunmehr 20 Jahren hat sich Transparency International dem Kampf gegen Korruption verschrieben. Inzwischen herrscht großes Einvernehmen über die Schädlichkeit der Korruption und der Bedeutung des Kampfes dagegen. Die Enthüllungen Edward Snowdens erinnern uns aber an die roten Linien, welche wir bei der Wahl der Mittel zur Korruptionsbekämpfung ziehen müssen.

Im Jahr 2009 sorgte der Deutsche Bahn-Skandal für Aufsehen. Ohne Wissen und Einverständnis wurden die Daten eines Großteils der Beschäftigten für eine sogenannte Massendatenanalyse genutzt, darunter auch die Bankdaten[26]. Dabei war es um das hehre Ziel der Betrugs- und Korruptionsbekämpfung gegangen. Transparency bezog klar Stellung:

> *»Die Verstöße der Deutschen Bahn AG gegen das Strafgesetzbuch (StGB), das Bundesdatenschutzgesetz (BDSG) und das Telekommunikationsgesetz (TKG) in der Vergangenheit waren geeignet, der Korruptionsbekämpfung und ihrer Akzeptanz erheblich zu schaden. Die Einhaltung des gesetzlichen Rahmens, die Einbindung der Belegschaft und ein vertrauensvolles Klima im Betrieb sind essentielle Voraussetzungen einer glaubwürdigen Korruptionsprävention.«*[27]

Dieses Beispiel zeigt, welche Grenzen auf nationaler Ebene gelten und gelten müssen. Allerdings wird es zunehmend schwierig auf nationaler Ebene zu regulieren. Im deutschen Strafprozessrecht wird vom Ideal der Aktenablage ausgegangen, also von Papier oder lokalen Rechnern, die in Geschäfts- oder Wohnräumen stehen[28]. Komplizierter wird die zügige Strafverfolgung korrupter Täter, wenn deren Informationen in transnationalen Netzwerken oder Clouds liegen. Eine solche

Vorgehensweise erleichtert korrupten Tätern, wenn sie es bewusst planen, Spuren zu verwischen[29].

Von diesem rechtmäßigen Vorgehen von Strafverfolgungsgehörden sind Spionageaktivitäten der Geheimdienste strikt zu trennen. Welche Grenzen müssen beim Wettbewerb der Staaten untereinander bzw. ihrer Unternehmen gelten? Zum Einsatz von Spionage zur Korruptionsbekämpfung gibt es zwar nur wenige Hinweise, aber diese sind eindeutig. Im Jahr 1995 berichtete[30] die Baltimore Sun, dass die NSA die Faxe und Telefonate zwischen dem europäischen Konzern Airbus und der saudischen Fluglinie und der saudischen Regierung abgehört habe und herausgefunden habe, dass die Airbusleute Bestechungszahlungen an saudische Amtsträger angeboten hätten. Diese Informationen wurden an US-Regierungsangehörige weitergegeben, so dass am Ende Boeing und McDonnell Douglas den 6 Mrd. Dollar Auftrag sicherten.

Noch bezeichnender ist der zweite Hinweis, denn es ist ein Geständnis des ehemaligen CIA-Chefs Woolsey, das im Jahr 2000 im Rahmen eines Gastkommentars im Wall Street Journal veröffentlicht wurde:

> *»Richtig, meine kontinentaleuropäischen Freunde, wir haben euch ausspioniert, weil ihr mit Bestechung arbeitet. Die Produkte eurer Unternehmen sind oftmals teurer oder technologisch weniger ausgereift als die eurer amerikanischen Konkurrenten, manchmal sogar beides. Deshalb besticht ihr so oft. [...] Wenn wir euch dabei erwischt haben – das mag euch vielleicht interessieren –, haben wir euren amerikanischen Konkurrenten kein Wort davon gesagt. Stattdessen wenden wir uns an die von euch bestochene Regierung und erklären deren Vertretern, dass wir diese Art von Korruption ganz und gar nicht gut finden. [...] Kommt wieder auf den Teppich, Europäer. Hört auf, uns Vorwürfe zu machen und reformiert eure etatistische Wirtschaftspolitik. Dann können eure Unternehmen effizienter und innovativer werden und müssen nicht mehr auf Bestechung zurückgreifen, um konkurrenzfähig zu sein. Und dann brauchen wir euch auch nicht mehr auszuspionieren.«*[31]

Wer Woolseys Zeilen liest, könnte vermuten, dass das gesamthafte Ausspionieren von Daten und Handlungen, Verstöße gegen den Datenschutz und die Missachtung verbriefter Bürgerrechte im Interesse einer wirksamen Korruptionsbekämpfung akzeptiert und hingenommen werden müsste. Dem ist aber nicht so. Niemals darf der Zweck die Mittel heiligen. Der Kampf gegen Korruption kann nicht gewonnen werden, wenn die Totalüberwachung dazu eingesetzt wird, Grundrechte zu verletzen, um wirtschaftliche Vorteile zu erlangen. Ebenso wird die Welt nicht sicherer und die Bevölkerung nicht wirksamer geschützt, wenn Persönlichkeitsrechte und die Pressefreiheit mit Füßen getreten werden.

Wir müssen Edward Snowden aber aus einem weiteren Grund dankbar sein. Dank seines Mutes und seiner Zivilcourage wurden wir erneut daran erinnert, wie schlecht es um den Schutz von Whistleblowern, insbesondere in Deutschland, bestellt ist. Zur erfolgreichen Korruptionsbekämpfung sind wir auf Whistleblower angewiesen. In einer Vielzahl von Fällen konnten Korruptionssachverhalte nur aufgedeckt werden, weil Whistleblower auf sie aufmerksam machten.

Bereits im Jahr 2009 hat Transparency International »27 Prinzipien für eine Whistleblower-Gesetzgebung«[32] veröffentlicht. Nach dem 8. Prinzip muss die Gesetzgebung dafür sorgen, dass auch Hinweise von außen, an Staatsanwaltschaften oder Medien, leicht gemacht werden. Die Möglichkeit, auch bei Enthüllungen in Bezug auf die nationale Sicherheit nach außen gehen zu können, wird im 9. Prinzip bewusst nicht ausgeschlossen.

Für Enthüllungen im Bereich der nationalen Sicherheit sind die »Tshwane Principles on National Security and the Right to Information« einschlägig. Sie wurden von rund 500 zivilgesellschaftlichen Akteuren, Sicherheitsexperten und Wissenschaftlern entwickelt und im Juni 2013 vom Rechtsausschuss der Parlamentarischen Versammlung des Europarates einstimmig unterstützt[33]. Die Öffentlichkeit hat danach ein Recht, über Überwachungsmaßnahmen informiert zu werden und zu erfahren, wer diese autorisiert hat.

In Deutschland ist es um den Schutz von Whistleblowern schlecht bestellt. Gleich mehrfach werden internationale Vorgaben von der Bundesregierung missachtet. Im G20-Aktionsplan vom November 2010 hat sich Deutschland verpflichtet, bis Ende 2012 Regeln zum Whistleblowerschutz zu erlassen und umzusetzen. Nichts geschah. Für eine Ratifizierung des Europarats-Zivilrechtsübereinkommens über Korruption muss der Hinweisgeberschutz im privaten Sektor verbessert werden. Dies hat auch die Parlamentarische Versammlung des Europarates im April 2010 gefordert. Nichts geschah. Auch die OECD-Konvention gegen die Bestechung ausländischer Amtsträger sieht effektiven Hinweisgeberschutz vor. Die Umsetzung der durch Deutschland ratifizierten Konvention erfolgt regelmäßig. Im sogenannten Phase 3-Bericht heißt es, dass Deutschland mehr tun muss, um Hinweise auf Korruption durch Unternehmensangehörige zu erleichtern, zum Beispiel durch einen besseren Schutz solcher Whistleblower. Nichts geschah. Im April 2013 hieß es im sogenannten Follow Up Bericht zum Phase 3-Bericht erneut, dass Deutschland mehr tun muss. Wieder geschah nichts. Dies ist international beschämend und stellt Deutschland in ein schlechtes Licht. Dabei gab es verschiedene Initiativen im Deutschen Bundestag. Kurz vor der parlamentarischen Sommerpause im Jahr 2013 wurden die entsprechenden Anträge der Oppositionsfraktionen reihenweise in wenigen Minuten abgelehnt. Im Halbrund des Deutschen Bundestages verloren sich vielleicht zwei Dutzend Abgeordnete, während gegenüber in der Deutschen Parlamentarischen Gesellschaft die Sektkorken knallten und die Abgeordneten feierten, dass endlich die Sommerpause losgeht.

Hinweisgeber wie Edward Snowden und viele andere sind zu schützen. Whistleblower sind auf Seiten der Machtlosen. Sie biedern sich gerade nicht bei den Mächtigen an. Diese Zivilcourage verdient jede Unterstützung.

Sicherheit vs.Privatsphäre?

Kirsten Fiedler

Die deutsche Regierung, die Geheimdienste, die Amerikaner, alle sind sich einig: Es muss eine Balance zwischen Privatsphäre und Sicherheit her. Manche sehen sie gar als dichotome Rivalen im Kampf gegen den Terrorismus oder behaupten, dies sei der zentrale Konflikt unseres Jahrhunderts.

Seit den ersten Leaks von Edward Snowden im Juni werden wir fast tagtäglich mit neuen schockierenden Details des Überwachungsskandals konfrontiert. Jeder Tag bringt neue Puzzlestücke über das Ausmaß der massiven Verletzung des Völkerrechts und der Privatsphäre aller Menschen, zu jeder Zeit. Dies führt nun zu einem Vertrauensbruch, der nicht nur einen erheblichen Schaden für die Informationsgesellschaft, sondern letztlich auch für die (hauptsächlich amerikanische) Wirtschaft[34] bedeutet.

Benjamin Franklin meinte schon zu seiner Zeit: »Diejenigen, die bereit sind grundlegende Freiheiten aufzugeben, um ein wenig kurzfristige Sicherheit zu erlangen, verdienen weder Freiheit noch Sicherheit.« Die Gegenüberstellung oder Suche nach dem Balanceakt Freiheit vs.Sicherheit ist einfach falsch. Es gibt keine Sicherheit ohne Privatsphäre. Unsere freien Gesellschaften bauen auf demokratischen Grundwerten auf. Demokratie wiederum setzt Meinungsfreiheit voraus, und Meinungsfreiheit und autonomes politisches Denken sind ohne Privatsphäre unmöglich. Ein Großangriff auf unsere Privatsphäre ist folglich eine Bedrohung für den Eckpfeiler aller Demokratien.

Michael Hayden, ehemaliger NSA-Chef, hingegen erklärt unermüdlich, dass die »amerikanische Gesellschaft zwischen Sicherheit und Freiheit wählen und eine Balance zwischen unserer Privatsphäre und unserer Sicherheit[35] gefunden werden muss. Auch US-Präsident Obama meint: »Man kann nicht 100 Prozent Sicherheit und 100 Prozent Privatsphäre

und null Unannehmlichkeiten haben«[36]. Nicht nur in den Vereinigten Staaten, auch hierzulande liest und hört man des öfteren, dass manche Praktiken gerechtfertigt seien, solange sie uns vor Terrorismus schützen.

Unser Bundesinnenminister Hans-Peter Friedrich beschwichtigt, dass unsere Privatsphäre für einen »edlen Zweck« geopfert wird. Aber Friedrich geht noch einen Schritt weiter. Nach einer Sondersitzung des Parlamentarischen Kontrollgremiums (PKGr) des Bundestags zum US-Überwachungsprogramm PRISM erklärte er, dass Sicherheit »Supergrundrecht« sei. Der neusprechblog erklärt, wie Friedrich hiermit das Grundrecht verdreht, indem er versucht es über andere Grundrechte zu stellen obwohl er eigentlich nicht die Sicherheit der Bürger meinte, sondern lediglich eine Rechtfertigung für die Überwachungsprogramme suchte. Eigentlich ginge es ihm darum, dass der Staat seine Bürger besser überwachen kann.

Auch manche EU-Gesetzentwürfe scheinen eher den Geheimdiensten und ihrer Datensammelwut zu helfen anstatt die Bevölkerung zu schützen. Zum Beispiel möchte die EU durch die im Februar 2013 vorgeschlagene NIS-Richtlinie für Netz- und Informationssicherheit auf kuriose Art und Weise den Umgang mit Datenpannen regeln. Datenlecks sollen den betroffenen Nutzern nicht direkt gemeldet werden. Im Gegenteil, Mitgliedstaaten sollen diese Pannen einem Netzwerk von (nicht genauer definierten) Behörden melden, die dann entscheiden, welche Sicherheitsverstöße eventuell den Nutzern gemeldet werden können oder ob sie sie einfach verschweigen. Professor Ross Anderson schreibt in einer lesenswerten Analyse[37], dass die Richtlinie ein Netzwerk aus nationalen Behörden schaffen soll, die Zugriff auf »ausreichende Informationen« von jedem überall haben sollen – was die Vorratsdatenspeicherung der Telekommunikationsdaten auf Suchmaschinen, Email und soziale Netzwerke erweitern würde. Hier geht es allein um die Sicherheit und das Fortbestehen des Sicherheitsapparates.

Aber wie sehr schützt uns die große Vielfalt der Sicherheitsmaßnahmen? Bei näherem Hinschauen entpuppen sie sich zumeist nicht nur als ineffizient sondern sind zudem – was viel gefährlicher ist – kontraproduktiv. Als konkrete Beispiele kann man hier unter anderem den elektronischen Personalausweis[38], die Vorratsdatenspeicherung[39], die Überwachung des Zahlungsverkehrs[40] oder auch Videoüberwachungsmaßnahmen[41] nennen. Die von unseren Regierungen gefeierten Erfolge sind häufig schlichtweg falsch oder basieren auf vorgegaukelten Bedrohungen (siehe »Anschläge, die keine waren«[42]). Und all dies im Namen der Kompromissfindung zwischen sicherheitspolitischen Anforderungen auf der einen Seite und der Privatsphäre auf der anderen.

Aber darf man sich überhaupt auf eine solche Debatte einlassen? Sicherheitsexperte Bruce Schneier kam vor einigen Jahren zu dem Schluss[43], dass es sich um eine falsche Diskussion handelt. Es ginge nicht um die Frage Privatsphäre vs.Sicherheit, sondern um Freiheit vs.Kontrolle. Wenn man eine falsche Dichotomie, ein falsches Dilemma, voraussetzt, wählt die Mehrheit verständlicherweise die Sicherheit.

Vielleicht sollten wir nicht über den unmöglichen Kompromiss zwischen Privatsphäre und Sicherheit diskutieren, sondern über das Gleichgewicht zwischen unserer individuellen Sicherheit und den nationalen Sicherheitssystemen.

Der Guardian veröffentlichte im September 2013 ein Dokument, welches belegt, dass sich die NSA gezielt darum bemüht, Verschlüsselungsstandards zu schwächen. Der amerikanische Sicherheitsdienst arbeitete an einer eigenen Version eines Entwurfs des Sicherheitsstandards des US National Institute of Standards and Technology, das für den weltweiten Einsatz in 2006 genehmigt wurde. Aus dem Budget der NSA für das Jahr 2013 ist zudem ersichtlich, dass Ressourcen dafür genutzt werden, um »politische Entscheidungen, Standards und Spezifikationen zu beeinflussen«[44].

Die Dienste verstoßen also mittlerweile direkt gegen Ziele des Allgemeinwohls indem sie unsere Sicherheit durch kontraproduktive Maßnahmen untergraben, systematisch Verschlüsselung knacken und schlechte Algorithmen verbreiten. Wie aber können wir uns weiterhin sicher fühlen, wenn Sicherheitsdienste weltweit außer Kontrolle geraten sind und das System untergraben, das uns schützen soll?

Die Cypherpunk-Bewegung hat in den 90er Jahren einen Anfang gemacht – jetzt müssen wir weiter dafür sorgen, dass Verschlüsselungstechnik, die auf offenen und freien Standards basiert, für alle zugänglich wird. Gleichzeitig muss das Recht auf Datenschutz endlich für jeden, für alle Bereiche und Situationen gelten, sonst kommt uns das Grundrecht abhanden. Bis wir eine volle Aufklärung des Überwachungsskandals haben, sollte die USA nicht weiterhin als Land gelten, das unseren Daten angemessenen Schutz bietet und daher alle Datentransfers unter dem »Safe Harbor«-Abkommen sofort eingestellt werden. Die neue Datenschutzverordung muss zukünftig regeln, dass Bürger_innen gewarnt werden, bevor sie Online-Dienste eines Landes benutzen, das keine ausreichenden Datenschutzstandards hat. Schließlich müssen die total veralteten Abkommen zwischen Geheimdiensten, die noch aus der Nachkriegszeit stammen, umgehend überprüft werden. Vor allem die UK/USA-Vereinbarung (Five Eyes) und der NATO-Vertrag müssen öffentlich diskutiert und grundlegend überarbeitet werden, um sie mit internationalen Menschenrechtsinstrumenten in Einklang zu bringen.

Ein Blick durchs PRISMa: Whistleblowing, Informationsmacht und mediale Kurzsichtigkeit

Arne Hintz

Die detaillierten Informationen über flächendeckende Internetüberwachung, die seit Anfang Juni 2013 zunächst im Guardian und der Washington Post (und später auch in anderen Medien) veröffentlicht wurden, haben unser Verständnis von Online-Kommunikation verändert. Wenngleich einiges von dem, was über den Whistleblower Edward Snowden und die Journalisten Glenn Greenwald und Laura Poitras den Weg in die Öffentlichkeit fand, schon vermutet wurde oder bereits Bekanntes ergänzte, liefern die ‘Leaks’ nun klare Beweise der Existenz umfassender staatlicher Überwachungs- und Spionageprogramme, die sich bis auf die Sabotage von Sicherheitsprogrammen und Eingriffen in Kommunikationsinfrastruktur erstrecken. Weder die beteiligten Regierungen, noch die Masse der Facebook-Nutzer/innen kann sich nun noch mit dem Verweis auf Verschwörungstheorien, die Verlässlichkeit demokratischer Staaten oder die inhärente Güte schicker New Economy Firmen herausreden.

Während uns Snowden wichtiges Wissen über die Kommunikationsplattformen geliefert hat, die wir täglich benutzen, bietet uns sein Fall auch Einsichten über breitere gesellschaftliche Trends. Schon WikiLeaks hatte uns neben den Informationen über Kriegsverbrechen und internationale Diplomatie eine Reihe weiterer Dynamiken verdeutlicht, die Politik, Medien und Gesellschaft betreffen und verändern. Als neuartige Medienorganisation hinterfragte es klassische Definitionen von Medien und Journalismus, verdeutlichte aktuelle Trends des Online-Aktivismus, und zeigte neue Formen der Internetzensur auf[45]. In der gleichen Weise bieten uns auch die Snowden-Veröffentlichungen eine Art Vergrößerungsglas, durch das

wir die Beziehungen zwischen Regierungen, Medien und anderen gesellschaftlichen Akteuren genauer betrachten und Veränderungen erkennen können. Im folgenden kurzen Beitrag möchte ich einige Beobachtungen darüber anstellen, was uns die Snowden Leaks – und die Reaktion auf ihre Veröffentlichung – jenseits der konkreten Erkenntnisse zur Internetüberwachung über weitere gesellschaftliche Themen sagen können. Insbesondere werde ich Medien, Journalismus und die Rolle von Whistleblowing ansprechen, zudem die Beziehungen zwischen Staat und Gesellschaft und die Debatte um Internetfreiheit. Die Perspektive auf diese Themen ist international, mit Fokus auf die Länder, auf die sich die Enthüllungen bislang konzentrieren – die USA und Großbritannien.

Medien und Journalismus

Bereits wenige Minuten nach dem Beginn der Veröffentlichungen trafen über Twitter die ersten Forderungen nach einem Pulitzer-Preis für Glenn Greenwald und die anderen beteiligten Journalisten ein. Gleichzeitig mit dem Erstaunen über die Informationen, die neues Licht auf staatliche Überwachung warfen, kam die Erkenntnis, dass es sich hierbei um einen herausragenden journalistischen Coup handelte. Guardian und Washington Post erklärten der Welt, was mit ihrer täglichen Telefon- und Internetkommunikation passiert, und wie der immer grösser werdende Teil unseres Lebens, der zunehmend untrennbar mit digitaler Kommunikation verbunden ist, überwacht und analysiert wird. Sie deckten geheime Regierungsprogramme und massive Eingriffe in die Privatsphäre auf, gegen den Widerstand ‘ihrer’ Regierungen. Die Veröffentlichungen sind somit ein Paradebeispiel für investigativen Journalismus und für die Rolle eines ‘Watchdogs’, der den Regierungen auf die Finger guckt und Fehlverhalten aufdeckt.

Die Monate nach dem Erscheinen der ersten Meldungen haben allerdings gezeigt, dass diese Watchdog-Rolle, die traditionell von der Presse gerne als Beweis ihrer Relevanz hochgehalten wird, eher eine Ausnahme ist als die Regel. Jenseits des Guardian war die Berichterstattung spärlich. Während das Thema in Deutschland aufgrund einer höheren Sensitivität bezüglich staatlicher Überwachung

noch etwas breiter diskutiert wurde, fand es anderswo kaum statt. Als etwa am 20. September aufgedeckt wurde, dass der britische Geheimdienst den belgischen Telekomanbieter Belgacom (der von EU-Behörden genutzt wird) nicht nur überwacht, sondern auch gehackt hat, war dies der BBC keine Meldung wert. Beiderseits des Atlantiks erweckten Medien eher den Eindruck, Online-Überwachung sei ein alter Hut und kaum der Aufregung wert[46]. Selbst nachweislich unrechtmässiges Verhalten wurde nur sehr vorsichtig, wenn überhaupt, kommentiert[47]. Das Interesse vieler Medien wechselte zudem schnell von der Nachricht zu ihren Überbringern und richtete sich auf Edward Snowden und Glenn Greenwald. Schon in Bezug auf WikiLeaks und Cablegate hatte die Strategie, vom eigentlichen Skandal abzulenken und sich stattdessen auf die Individuen zu konzentrieren, gut funktioniert. Nicht die aufgedeckten Kriegsverbrechen, Regierungspionage und weitere Skandale hatten den grössten Teil der medialen Debatte bestimmt, sondern die Eigenarten von Julian Assange und das Privatleben von Bradley Manning[48].Zur Kritik an Whistleblowern und einzelnen Journalisten gesellten sich zudem Angriffe auf jene Medienorganisationen, die über die Leaks berichteten. So attackierten Zeitungen wie etwa die Times und der Daily Telegraph den Guardian, der mit seinen Veröffentlichungen die Sicherheit des Landes gefährdet habe, und machten sich so zum Sprachrohr der konservativen Regierung und der Spionagebehörden.

Die Art der Berichterstattung bestätigte die vielfach erforschten Mängel in der medialen Aufarbeitung staatlichen Fehlverhaltens (siehe z.B. [49]). Snowden selbst hatte diese Bedenken geteilt: Er erklärte zu Beginn der Enthüllungen, dass er sich nicht an die New York Times gewandt hatte, da sie die Veröffentlichung ähnlicher Leaks 2003/04 verzögert hatte (bis nach der damaligen amerikanischen Präsidentenwahl). Auch die Washington Post veröffentlichte Snowdens Informationen erst, als mit dem Guardian eine weitere Zeitung einbezogen wurde, die eher dazu bereit war. Aus dem Bild des ‘Watchdogs’, also der öffentlichen Überwachung der Regierungsarbeit, wird somit nicht nur das des

‘Lapdogs’, also des Schosshündchens von Regierungen. Diese Haltung wurde wunderbar von dem britischen Journalisten Chris Blackhurst ausgedrückt, der ernsthaft die Frage stellte, was ihm als Journalist denn das recht gebe, die Arbeit der staatlichen Sicherheitsbehörden zu hinterfragen[50]. Dass genau dies sein Job ist, scheint keine besonders weit verbreitete Meinung mehr zu sein (wenngleich der Guardian von renommierten internationalen Zeitungen zumindest verbal Unterstützung erfuhr).

Die medialen Reaktionen zwischen Totschweigen und Angriffen auf investigativen Journalismus gehen jedoch weit über das Konzept des harmlosen Schoßhündchens hinaus. Sie bedeuten nicht nur eine mangelhafte Ausführung journalistischer Arbeit, was lediglich ein bedauernswertes Defizit wäre, sondern vielmehr eine aktive Unterstützung geheimer Regierungsprogramme gegen BürgerInnen und Zivilgesellschaft. Erst als mit dem Abhören von Angela Merkel und anderen Regierungschefs Regierungen selbst betroffen waren, führte dies zu breiterer Berichterstattung und ernsterer Mediendebatte.

Kaum thematisiert wird dabei auch, dass journalistische Arbeit von flächendeckender Kommunikationsüberwachung fundamental infrage gestellt wird. Investigativer Journalismus, der Skandale aufdeckt und das öffentliche Interesse gegen einflussreiche Akteure schützt, basiert auf vertraulicher Kommunikation mit Quellen. Wenn diese Vertraulichkeit nicht mehr gewährleistet ist, ist nicht nur die Sicherheit der Quellen, sondern diese Art von Journalismus insgesamt gefährdet[51].

So wie bereits der WikiLeaks-Fall sagt uns auch der Snowden-Fall nicht nur etwas über die Qualität journalistischer Arbeit, sondern auch über die strukturelle Entwicklung der Medienlandschaft. Neben dem traditionellen »fourth estate« bzw. der vierten Gewalt, also der klassischen Presse, gewinnt der »fifth estate« bzw. die fünfte Gewalt an Bedeutung. Dazu zählen neue nicht-professionelle Medienakteure, »citizen journalists« und Medienaktivist/innen. Der amerikanische Wissenschaftler Yochai Benkler hat all diese Akteure in seiner Idee eines

»networked fourth estate« zusammengefasst[52]. Hierzu gehören die klassischen Medien, aber auch Nichtregierungsorganisationen, Communitymedien, Blogs, und neue Informationsplattformen wie etwa WikiLeaks.

Whistleblowing

In einer Medienumgebung, die einerseits von neuen Medienakteuren und andererseits von ökonomischen Krisen (und, damit verbunden, der Verkleinerung von Redaktionen) geprägt ist, erhalten Whistleblower verstärkte Relevanz als Quellen wichtiger Informationen. Zudem ermöglicht die technologische Entwicklung die Speicherung und Weitergabe von Daten und beeinflusst damit, was geleakt werden kann (große Datenmengen), wo es veröffentlicht wird (z.B. WikiLeaks und andere Internetplattformen) und wer ein Whistleblower werden kann. Während Daniel Ellsberg vor 40 Jahren noch die Pentagon Papers Seite für Seite fotokopieren musste, konnte Bradley Manning hunderttausende Dokumente auf eine CD-ROM kopieren und sie als Musik-CD getarnt aus einer Militärbasis schaffen. Geschätzte 2-3 Millionen Armee- und Regierungsangestellte hatten regelmässig Zugang zu den Dokumenten, die anschliessend von WikiLeaks und Partnerorganisationen u.a. in den »Cablegate«-Depeschen veröffentlicht wurden, und für deren Weitergabe Manning später zu 35 Jahren Haft verurteilt wurde[53]. Snowden war lediglich bei einer Vertragsfirma beschäftigt und hatte trotzdem Zugang zu Dokumenten, die internationale Skandale aufdeckten, diplomatische Verwerfungen auslösten und zu einer internationalen Hetzjagd auf den Whistleblower führten.

Für traditionelle Medien brachten jene neuen Whistleblower neue Herausforderungen, einschliesslich der praktischen Notwendigkeit sicherer (also verschlüsselter) Online-Kommunikation. Eine der problematischsten Erkenntnisse aus der WikiLeaks-Saga von 2010 war wohl die Sorglosigkeit und Amateurhaftigkeit mit der Journalisten und Chefredakteure der renommiertesten Zeitungen der Welt auf das

Bestreben von WikiLeaks reagierten, sicher zu kommunizieren und Daten zu verschlüsseln (siehe u.a. [54]).

Das Imperium schlägt zurück

Die Reaktion darauf ist ein beispielloses Repressionsprogramm gegen Whistleblower. Die Obama-Regierung hat mehr Whistleblower straftrechtlich verfolgt als alle vorherigen US-Administrationen zusammen. Der »Krieg gegen die Whistleblower« beschränkt sich nicht auf die prominenten Fälle von Bradley Manning und Edward Snowden, sondern soll allgemein die Informationskontrolle steigern und als Abschreckung gegen unerlaubte Informationsweitergabe dienen. Das »Insider Threats Program« etwa, das sich auf alle Bereiche der US-amerikanischen öffentlichen Verwaltung erstreckt, in denen sensitive Daten behandelt werden, soll systematisch erfassen, welche Mitarbeiter ein mögliches Risiko bezüglich der Datenkontrolle darstellen. Jegliches »verdächtige« Verhalten von Kollegen muss an Vorgesetzte gemeldet werden[55]. In Grossbritannien kommt weiterhin der »Official Secrets Act« zur Anwendung, ein Gesetz, das aus dem Jahr 1889 stammt (wenn auch mit einigen Veränderungen) und aufgrund dessen immer noch Whistleblower angeklagt werden, beispielsweise 2007 ein Parlamentsangestellter, der geplante militärische Angriffe auf Journalisten während des Irakkriegs öffentlich gemacht hatte[56].

Das Verfahren gegen Bradley Manning zeigte deutlich, wie rigoros die staatliche Reaktion auf unerlaubte Datenweitergabe ist. Der Whistleblower, der Kriegsverbrechen, Korruption und Spionage öffentlich gemacht hatte, wird den grössten Teil seines Lebens hinter Gittern verbringen, während Julian Assange im equadorianischen Konsulat in London festsitzt, Snowden in Russland, und alle drei des Öfteren als Terroristen bezeichnet werden, denen (nach Meinung einiger amerikanischer Politiker) die gleiche Behandlung zuteil kommen sollte wie Osama Bin Laden. Staatliches Fehlverhalten aufzuzeigen gilt mittlerweile als Terrorismus und das spürt auch die traditionelle Presse. Als im August 2013 David Miranda im Auftrag des Guardian unterwegs

war und bei seiner Zwischenlandung in London Heathrow neun Stunden lang zum Snowden-Fall verhört wurde, geschah dies auf Basis britischer Anti-Terror-Gesetze. Kurz vorher waren bereits britische Agenten in den Redaktionsräumen des Guardian aufgetaucht und hatten (erfolgreich) verlangt, dass Festplatten zerstört würden, auf denen Dateien aus dem Snowden-Fundus gelagert waren. Interessant ist bei diesen Fällen nicht nur, dass sie passieren, sondern auch die Selbstverständlichkeit, mit denen staatliche Behörden Anti-Terror-Gesetze ausdehnen und in die Pressefreiheit eingreifen und dabei kaum öffentlichen Gegenwind erwarten. Selbst der Guardian berichtete erst mit mehrwöchiger Verspätung über den Einsatz in seiner Redaktion und die Zerstörung seiner Computer.

Ist Information Macht?

Die unverhältnismässige Repression gegen Informationsweitergabe scheint die alte These zu bestätigen, wonach Information Macht ist. Zuletzt hatte der renommierte Wissenschaftler Manuel Castells mit seinem Buch »Communication Power« die vielfältigen Verbindungen zwischen beidem herausgearbeitet[57]. Die Obama-Regierung verdeutlicht die Aktualität dieses Ansatzes sehr anschaulich durch ihr extremes Bemühen um Informationskontrolle. Dabei hatten die Erfahrungen von WikiLeaks nicht zuletzt auch die Grenzen von Informationsstrategien aufgezeigt. Der ursprüngliche Ansatz, Rohdaten auf einer Internetplattform für alle zugänglich zu veröffentlichen, war nur von einem kleineren Publikum wahrgenommen und genutzt worden. Die darauf folgende Strategie der Zusammenarbeit mit namhaften Medien erweiterte zwar den Kreis derer, die über die Dokumente erfuhren, doch die weltweite Debatte und der tiefgreifende Politikwechsel, die Bradley Manning sich erhofft hatte, fanden nur sehr begrenzt statt[58]. Sowohl der WikiLeaks-Fall als auch die Snowden-Erfahrung zeigen, dass Information allein kaum unmittelbaren sozialen und politischen Wandel herbeiführt, solange die Deutungshoheit bei etablierten gesellschaftlichen Kräften liegt. Allerdings lassen die Reaktionen vieler Regierungen darauf schliessen, dass Informationen durchaus eine Gefahr für die Sicherung der herrschenden Verhältnisse

darstellen. Diese Gefahr bezieht sich weniger auf konkrete kurzfristige Politik (wie etwa die Fortführung eines Krieges), sondern eher auf die langfristige Legitimation von Regierungspolitik und das Verhältnis zwischen Politik und Gesellschaft.

Staat und Gesellschaft

Die flächendeckende Überwachung der Internetkommunikation verändert das Verhältnis von Staat und Gesellschaft nachhaltig. Überwachung verändert menschliches Verhalten, untergräbt kritische Auseinandersetzungen (und somit das Wesen der Demokratie) und hebelt die Unschuldsvermutung aus. Die Privatsphäre »unterliegt automatisch einer Art Staatsvorbehalt«[59] und wird dadurch fundamental eingeschränkt.

Staatliche Aktivität findet dagegen zunehmend im Geheimen statt. Demokratische Kontrolle wäre gerade bei geheimen staatlichen Prozessen notwendig, findet aber in den von Snowden aufgedeckten Fällen kaum statt. Die FISA Gerichte in den USA haben keine nennenswerte Kontrollfunktion ausgeübt und stellten sich eher als pseudodemokratisches Feigenblatt dar[60], und in Grossbritannien behaupten selbst Mitglieder der relevanten parlamentarischen Kontrollgremien, nichts von PRISM und Tempora gewusst zu haben[61]. Aus demokratischen Prozessen und Institutionen werden so geheime Parallelwelten, was für die Zukunft demokratischer Staaten noch weit tiefergehende Folgen haben kann als die eigentliche Überwachung.

Selbst wenn die Beteuerungen der Regierungen, es handle sich bei der Online-Überwachung um eingeschränkte und demokratisch kontrollierte Maßnahmen zur Terrorabwehr dem Wunsch vieler Menschen entsprechen mag, sich nicht weiter mit dem Thema zu beschäftigen, so haben sich viele Regierungen doch ein Vertrauensproblem eingehandelt. Zu offensichtlich und zu unüberbrückbar ist der Gegensatz zwischen den Beschwichtigungen von Regierungsseite und der Tatsache, dass die Überwachung gerade nicht auf bestimmte Personen, sondern auf die breite Masse der Facebook-

User und Emailenden abzielt. Gerade in Deutschland ist die Sensibilität bezüglich flächendeckender Überwachung groß und hat seit Jahren zu großen Protesten gegen die Vorratsdatenspeicherung geführt. Aber auch in Großbritannien und anderswo verbreitert sich im gesellschaftlichen Mainstream die Einsicht, dass die eigene Regierung nicht unbedingt im besten Interesse von Demokratie und Freiheit handelt[62]. Nachdem der Überwachungsskandal lange Zeit von der britischen Politik mit weitgehender Nichtbeachtung behandelt wurde, führten öffentlicher Druck und Risse in der liberal-konservativen Regierungskoalition im Oktober 2013 zur Einberufung einer parlamentarischen Untersuchungskommission, die sowohl das Ausmaß der Internetüberwachung als auch die demokratische und rechtliche Kontrolle der Sicherheitsbehörden kritisch beleuchten soll[63].

Internet

Online-Kommunikation ist selbstverständlich am vielfältigsten von den Überwachungsprogrammen beeinflusst, doch auch hier zeigen die Snowden-Enthüllungen längerfristige Trends und historische Momente auf. Zum einen verdeutlichen sie einmal mehr das Ende des grenzenlosen und offenen Cyberspace. Ähnlich den immer weiter verbreiteten Filtern und Contentblockern deutet auch die Überwachung auf die Existenz von Grenzen im Cyberspace und auf die tiefen Eingriffe von Regierungen und Behörden in die freie Kommunikation. Bereits vor mehreren Jahren hatten Wissenschaftler wie Goldsmith und Wu betont, dass das grenzenlose Internet ein Mythos sei[64] und dies wird nun einmal mehr bestätigt.

Zweitens räumen die Enthüllungen mit den neuen Kalten-Kriegs-Szenarien auf, die sich in den vergangenen Jahren stark verbreitet hatten. Zugespitzt durch Hillary Clintons Rede über Internetfreiheiten im Jahr 2010[65] hatte sich in Regierungen, internationalen Institutionen, aber auch Teilen der Wissenschaft und Zivilgesellschaft ein Diskurs herausgebildet, der den demokratischen Westen mit seinen Kommunikationsfreiheiten dem autoritären Osten mit seinen

Netzfiltern und Überwachungsprogrammen entgegenstellte. Mit PRISM und Tempora können diese Überlegungen nun ad acta gelegt werden. Und drittens heben die Snowden-Leaks – wie schon zuvor die WikiLeaks-Enthüllungen – die problematische Rolle privater Internetfirmen hervor. War es bei WikiLeaks vor allem die Ressourcenblockade von Webspace- und Finanzanbietern wie etwa Amazon und Paypal, die die Interventionen kommerzieller Dienste verdeutlichte, so rücken nun bei der Online-Überwachung die grossen Konzerne sozialer Medien in den Blickpunkt. Google, Facebook, etc. stehen im Zentrum der Überwachungspraktiken und arbeiten eng mit Regierungsstellen zusammen. Mit PRISM und Tempora zeigen sich schlagartig die Probleme unserer alltäglichen Kommunikationspraktiken, die immer stärker auf den Diensten dieser Konzerne beruhen.

Veränderung

Die Snowden-Enthüllungen helfen uns, aktuelle Entwicklungen und längerfristige Trends zu beobachten und zu erkennen. In diesem Kapitel habe ich mich insbesondere mit Tendenzen in Medien und Journalismus beschäftigt. Mit den Leaks können wir die Stärken und Schwächen des Mediensystems beleuchten, sowie strukturelle Veränderungen erkennen. Doch auch Dynamiken in der Internetkommunikation und im Verhältnis von Staat und Gesellschaft können die Enthüllungen aufzeigen.

Angesichts des Umfangs der Überwachung, staatlicher Repression und öffentlicher Lethargie scheint wenig an den neuen Realitäten, die von den Leaks beschrieben wurden, zu rütteln. Allerdings bieten die positive Beispiele des investigativen Journalismus Grund für vorsichtigen Optimismus. Die verschiedenen Abschreckungsversuche gegen potenzielle Whistleblower – einschliesslich der Behandlung von Bradley Manning – haben zumindest bei Edward Snowden nicht gewirkt, und die implizite Anerkennung der Informationsmacht der »fünften Gewalt« bietet Anknüpfungspunkte. Öffentliche Kampagnen, wie z.B. gegen die Vorratsdatenspeicherung, dürften sich eher vergrößern, neue Kampagnen wie etwa »Stop Watching Us« werden gegründet und haben zu ersten Groβdemonstrationen geführt, und selbstorganisierte

Kommunikationsplattformen und Anonymisierungstools werden seit Snowdens Enthüllungen stärker nachgefragt. Wenn die Leaks ein Wendepunkt hin zu einem kritischeren Umgang mit sowohl sozialen Medien als auch Regierungsverlautbarungen sind, dann ist auch dies ein historischer Moment.

Minority Reports 'Precrime' ist das Ziel des MI5 Director General Andrew Parker

Jan-Peter Kleinhans

Der gegenwärtige Director General des britischen Geheimdienstes MI5, Andrew Parker, hielt am 8.10.2013 die erste offizielle Rede in seiner Amtszeit[66]. Dabei hat er natürlich vor allem von den Gefahren gesprochen, die seine Institution versucht abzuwehren und wie viel Schaden Snowdens Veröffentlichungen angerichtet haben. Mittendrin findet man dann jedoch, was er sich eigentlich für den MI5 wünscht:

> *»In einem gewissen Sinne ist Terrorismusbekämpfung eine außergewöhnliche Angelegenheit. Lassen Sie mich sagen, was ich meine. Terrorismus ist, aufgrund seiner Natur und der Folgen, der einzige Bereich der Kriminalität, wo die Erwartung manchmal zu sein scheint, dass die Statistik Null sein sollte. Null. Stellen sie sich vor, das selbe Ziel würde auf Mord im Allgemeinen oder organisierten Drogenhandel angewendet werden. Das kennt man nur von 'Precrime' aus dem Tom Cruise Film 'Minority Report'. Das Leben ist nicht wie im Film. In einer freien Gesellschaft ist Null, angesichts der anhaltenden und ernsthaften Bedrohungen, natürlich unmöglich zu erreichen – jedoch werden wir weiterhin danach streben.«*

Was sagt Andrew Parker da eigentlich? Die Gesellschaft erwartet seiner Meinung nach, dass Terror-Anschläge immer verhindert werden – im Gegensatz zu Mord oder organisiertem Drogenhandel. Parker sagt nicht, dass etwas wie Precrime unmöglich wäre – ganz im Gegenteil. Er sagt, dass ein hundertprozentiges Vereiteln von Terror-Anschlägen in einer *freien* Gesellschaft, die ständig von außen und innen bedroht wird, unmöglich sei – dass MI5 sich aber bemüht, dieses Ziel der hundertprozentigen Sicherheit vor Terror-Anschlägen zu erreichen.

In Philip K. Dicks Kurzgeschichte *Minority Report* – welche die Grundlage des gleichnamigen Films ist – gab es in der Gesellschaft schon seit 5 Jahren keinen Mord mehr. Allen geht es »gut«. In *Minority Report* wird diese praktisch hundertprozentige Sicherheit vor Morden durch hundertprozentige Kontrolle der Bürger ermöglicht. Wenn man nur an einen Mord denkt oder im Affekt ein Verbrechen begehen will, wird man verurteilt. Das scheint wirklich sehr weit entfernt von unserer jetzigen Gesellschaft. Und doch ist es das gar nicht. Andrew Parker sagt ganz deutlich, dass sein Ziel für den MI5 möglichst vollständige Prävention von terroristischen Aktivitäten ist. Und dieses Ziel versucht er – ganz ähnlich zu Dicks Vision – durch vollständige Kontrolle jeglicher Kommunikation zu erlangen. Die zunächst freie Gesellschaft muss also – zu ihrem eigenen Wohl – kontrolliert werden, damit ihre Sicherheit besser gewährleistet werden kann. Anders als im Film geschieht diese Kontrolle nicht durch drei Frauen in Nährlösung und Holzkugeln, sondern durch all die Dinge, die Snowden in den letzten Monaten veröffentlicht hat: Globale Überwachung jeglicher Telekommunikation, Abspeicherung in riesigen Datenzentren und anschließende Analyse – all das mit dem Ziel, möglichst viel zu wissen.

Natürlich hat Parker im weiteren Verlauf der Rede immer wieder versucht, zu beteuern, dass weder MI5 noch GCHQ willkürlich die Gesellschaft beobachten und somit unter Generalverdacht stellen.

> *»Ich bin sehr froh, dass wir eine enorm rechenschaftspflichtige Behörde sind ... Wir zeigen Beweismittel vor Gericht ...”*

Andrew Parker spricht hier zwar für den MI5, für die Tochter-Behörde GCHQ ist beides jedoch keineswegs der Fall. Erst eine Woche vor seiner Rede kamen Ben Scott und Stefan Heumann in ihrer Studie[67] zur rechtlichen Lage der US-amerikanischen, britischen und deutschen Geheimdienstgesetze zu dem Schluss, dass Großbritannien die schwächsten Kontrollmechanismen hat und den Geheimdiensten die größten Freiheiten einräumt. Zur umfassenden Überwachung der Telekommunikation benötigen die britischen Geheimdienste gerade

keine richterliche Bevollmächtigung, sondern lediglich ein »Zertifikat« des Innenministers.

> *»Wir wollen nicht den alles durchdringenden, repressiven Überwachungsapparat ... Die Realität der täglichen geheimdienstlichen Arbeit ist, dass wir unsere intensivste und aufdringlichste Aufmerksamkeit ausschließlich einer kleinen Zahl an Fällen zu jeder Zeit widmen. Die Herausforderung liegt darin, Entscheidungen zwischen mehreren konkurrierenden Anforderungen zu treffen, um uns die beste Chance zu geben, zur richtigen Zeit am richtigen Ort zu sein um Terrorismus zu verhindern. Und lassen Sie mich das klarstellen – wir setzen Maßnahmen mit einem schweren Eingriff in die Privatsphäre nur bei Terroristen und jenen ein, die die Staatssicherheit gefährden. Das Getz verlangt, dass wir Informationen nur sammeln und auf diese zugreifen, wenn wir sie wirklich für unsere Arbeit benötigen, in diesem Falle zur Bekämpfung der Bedrohung durch Terrorismus.«*

Das hört sich natürlich zunächst sehr beruhigend an. Selbst der Direktor des MI5 ist gegen allgegenwärtige und allmächtige Überwachung. MI5 agiert innerhalb der engen Schranken des Gesetzes. Wenn man sich jedoch die Frage stellt, wie MI5 und GCHQ überhaupt Terroristen identifizieren, ergibt sich ein anderes Bild: Um einen Terroristen zu verfolgen, muss man zunächst wissen, ob es sich um einen Terroristen handelt. Da jegliche Telekommunikation potenziell terroristischer Natur sein könnte, muss man – folgerichtig – auch jegliche Kommunikation überwachen. Da man zur Zeit zwar die Möglichkeiten hat, jegliche Kommunikation mitzuschneiden und zu speichern, die Analysemöglichkeiten und Algorithmen aber noch sehr limitiert sind – außerdem braucht es Zeit, um Verschlüsselungen zu knacken[68] – ging man in den letzten Jahren dazu über, alles in riesigen Datenzentren abzuspeichern[69]. Was in Parkers Rede als sehr bedacht, fokussiert und limitiert dargestellt wird, ist in Wahrheit viel näher an der ‘Gedankenkontrolle’, die in Dicks Kurzgeschichte *Minority Report* beschrieben wird: Wenn die Regierung die Kriterien für ‘Terrorismus’ festlegt und die Kommunikation ihrer Bürger über Jahrzehnte

abspeichert, ist die Bevölkerung der Willkür zukünftiger Regierungen schutzlos ausgeliefert. Was heute noch legaler Protest ist, könnte in wenigen Jahren schon als terroristischer Akt begriffen werden. Und da alles festgehalten wurde und die jeweilige Regierung vollständigen Einblick hat, hat sie auch vollständige Kontrolle über die Bevölkerung.

Die Rhetorik, der sich Parker bedient, setzt zwar die Freiheit der Bürger der Sicherheit der Gesellschaft gegenüber. Darum geht es aber nicht. Es geht um Kontrolle. In welchem Ausmaß kann die Regierung die Bevölkerung kontrollieren?

> *»Der MI5 wird weiterhin die Fähigkeit benötigen, die Kommunikation von Terroristen zu überwachen, wenn uns das ermöglicht, ihre Absichten zu kennen und sie zu stoppen. Das Gegenteil dazu wäre, zu akzeptieren, dass Terroristen Möglichkeiten zur Kommunikation haben, bei denen sie sicher sein können, dass sie außerhalb der Überwachungsmöglichkeiten des MI5 oder GCHQ liegen – basierend auf unseren gesetzmäßigen Befugnissen. Glaubt das tatsächlich irgendjemand?«*

Parkers Aussage kann man als offizielle Begründung lesen, warum Polizei und Staatsanwaltschaft in Großbritannien Passwörter zu verschlüsselten Datenträgern oder Accounts von Verdächtigten verlangen dürfen: Es darf keinen Kommunikationskanal geben, der nicht der staatlichen Überwachung unterliegt, denn dieser könnte durch Terroristen ausgenutzt werden. Parker gibt hier wieder ein Beispiel für die vorherrschende Überzeugung, dass nur durch vollständige Kontrolle aller Kommunikationswege Sicherheit erlangt werden kann. Ein weiterer rhetorischer Kniff kommt am Ende der Rede:

> *»Abschließend möchte ich Sie an etwas erinnern, das allzu leicht vergessen wird. MI5 ist am Ende eine Organisation aus Mitgliedern der Öffentlichkeit aus allen Bereichen des Lebens, die es sehr wichtig nehmen in was für einer Art von Land wir leben. Das ist der Grund, weswegen sie dort arbeiten.«*

Parker bemüht hier aus gutem Grund das Bild, dass in den Geheimdiensten Bürger mit den besten Absichten und reinsten Motiven

arbeiten, die im Dienste ihres Landes stehen. In den vergangenen Wochen haben die Schlagzeilen vor allem dafür gesorgt, dass Geheimdienste als »Eindringlinge« in die Privatsphäre der Bürger empfunden wurden. Daher der verständliche Versuch Parkers, Geheimdienste als Teil der Gesellschaft zu porträtieren. Das ändert jedoch nichts an der Tatsache, dass die vollständige Abschottung der Geheimdienste und ihre Verschwiegenheit einheitliches Denken und sich selbst verstärkende Ideologien provoziert. Dies führte dazu, dass Whistleblower, wie Thomas Drake oder Edward Snowden, mit interner Beschwerde nicht weiterkamen, da sie »aus der Reihe tanzten« – und das mag man nicht. Andersdenken und Hinterfragen wird in solchen Institutionen systemisch verhindert.

Letztlich bedient sich Andrew Parker in seiner Rede einer Vielzahl von Rhetoriken, die man zum Teil aus »War on Terror«[70] kennt: Das Bild der konstanten und unmittelbaren Gefahr durch Nicht-Bürger – Terroristen – wird verstärkt. Die Überwachungsinfrastruktur wird als einziges Mittel dargestellt, um diese Gefahren abzuwehren. Im Fokus steht Abwehr – nicht Überwachung. Und der direkte Zusammenhang zwischen »mehr Daten« bedeutet »mehr Sicherheit« wird betont. Andrew Parkers unterschwellige Botschaft: Sollte irgendetwas am Status Quo geändert werden, wird dadurch sofort die nationale Sicherheit gefährdet – daher werden Whistleblower und deren Veröffentlichungen als ernsthafte Gefahrenquelle für die gesamte Gesellschaft dargestellt. Was auch prompt durch einschlägige englische Tageszeitungen aufgegriffen wurde. So berichteten vor allem die britischen Tageszeitungen über die angeblichen Gefahren für die Gesellschaft, die Parker in seiner Rede immer wieder erwähnte: Edward Snowden habe den Terroristen ein Geschenk gemacht.

Man sollte versuchen, nicht denselben Fehler wie Daily Mail, The Daily Telegraph oder The Times zu begehen. Googles Amit Singhal hatte in einem Interview[71] gegenüber dem Slate Magazine gesagt, dass Googles Ziel sei, Antworten zu liefern, bevor man fragt. Predictive Search.

»Ich kann mir eine Welt vorstellen, in der ich gar nicht mehr suchen muss. Ich bin nur irgendwo draußen am Mittag und meine Suchmaschine empfiehlt mir sofort Restaurants in der Nähe, die mir gefallen werden, da ich scharfe Gerichte mag.«

Im Falle von Google ist das Resultat mehr Komfort für den Benutzer. Dieselbe Idee haben natürlich auch die Geheimdienste – ansonsten würden nicht riesige Datenzentren gebaut werden oder intensive Kooperationen mit US-amerikanischen Hochschulen eingegangen werden. Keith Alexander, Direktor der NSA, hatte Anfang August gesagt, dass die NSA 90% der System-Administratoren entlassen will - um die Arbeit durch verlässliche Algorithmen erledigen zu lassen. Das macht Sinn, da das Kerngeschäft der Geheimdienste das Abfangen, Filtern und Analysieren von Datenflüssen ist. Dafür benötigt es potente Hardware und Entwickler – wie bei Google. Vor allem jedoch schlaue Algorithmen, die ständig dazulernen, Muster erkennen und mit möglichst vielen Daten gefüttert werden. Das Resultat für den Bürger ist jedoch keinesfalls mehr Komfort. Das Resultat wurde durch Philip K. Dick beschrieben und Andrew Patrick hat durch viele der Aussagen seiner ersten Amtsrede diesen Eindruck nochmals untermauert: Vollständige Kontrolle aller Kommunikationskanäle, basierend auf dem Glauben, dass dadurch Sicherheit vor Systemkritikern und Andersdenkenden erlangt wird. Deswegen wird die konstante Bedrohung der Gesellschaft betont und nicht darüber gesprochen, dass durch Kontrolle natürlich auch Machterhalt der Institutionen und der Status Quo sichergestellt werden. Deswegen wird der fragwürdige Zusammenhang zwischen Kommunikationsüberwachung und Verbrechensprävention nicht hinterfragt. Deswegen wird nicht darüber gesprochen, dass allein die bisher über uns gespeicherten Daten ein reales Risiko darstellen, falls eine der nächsten Regierungen – ganz gleich ob in Deutschland, Großbritannien oder den USA – ein anderes Terrorismus-Verständnis hat.

Es ging nie um die Abwägung von Freiheit gegenüber Sicherheit. Es geht ausschließlich um Kontrolle. Vollständige Kontrolle der Bevölkerung durch umfassende, verdachtsunabhängige Überwachung jeglicher

Kommunikation. Sicherheit kann ein Nebeneffekt von Kontrolle sein – muss es aber nicht. Kontrolle fokussiert immer auf Machterhalt und Abschottung nach außen.

Eine kontrollierte Gesellschaft kann niemals frei sein.

Wie ‘Sicherheit’ unsere Gesellschaft gefährdet

Gabriella Coleman

Aus all den Vorwürfen, mit denen Edward Snowden bombardiert wurde, empfinde ich die laienhafte Diagnose seines »Narzissmus« am rätselhaftesten und unberechtigsten. Was ist daran narzisstisch, sein Leben zu riskieren – und mit Leben meine ich ein Leben im Gefängnis? Obwohl er, teilweise zum Selbstschutz, an die Öffentlichkeit ging, hat er seine Interaktion mit den Medien auf das Mindeste reduziert und ganz offensichtlich keine unnötige Aufmerksamkeit gesucht. Aufgrund der mangelnden Beweise für solch eine Diagnose scheint es sich eher um Rufmord zu handeln, um von den dringenderen Problemen abzulenken, die durch seine Taten enthüllt wurden.

Wenn wir das, was er tat nicht mit seiner Persönlichkeit, sondern mit dem gegenwärtigen historischen Moment in Zusammenhang bringen, sehen wir ohne jeglichen Zweifel, dass Edward Snowden nicht allein ist. Er ist Teil einer wachsenden Schar an Bürgern, die seit Jahren erkannt haben, dass der explosionsartige Anstieg staatlicher Geheimhaltung und Überwachung solch ein großes Problem ist, dass sie gewillt sind, persönliche Risiken einzugehen, um eine Debatte und einen Umbruch voranzutreiben. Am bemerkenswertesten ist, dass sich diese Schar aus Insidern (William Binney, Thomas Drake, Edward Snowden, Bradley Manning) und Outsidern (Julian Assange, Barrett Brown, Laura Poitras, James Bamford) zusammensetzt. Es ist bemerkenswert, dass ihre Kernaussagen die selben sind.

Die Öffentlichkeit sollte vielleicht skeptischer sein, wenn es sich nur um eine Person handeln würde oder um die Julian Assanges dieser Welt – Langzeit-Aktivisten, die seit jeher außerhalb des staatlichen Apparates sitzen – die aufschreien. Dass wir investigative Journalisten, Militärpersonal, Mitarbeiter von Sicherheitsbehörden und Aktivisten haben, die sich dem Schlachtgetümmel anschließen, verdeutlicht das Ausmaß des Problems. Unterschiedliche Individuen ohne jegliche

Verbindung, aus verschiedensten gesellschaftlichen Schichten treten hervor und identifizieren ähnliche Probleme.

Dies bringt uns zu den Ufern des zweiten Problems: Die Unverletzlichkeit des Gesetzes. Ich denke, nun ist offensichtlich, dass die enthüllten Programme Teile des Gesetzes verletzen – sowohl im Wortlaut als auch im Geist. Anwälte haben es erst kürzlich unmissverständlich ausgedrückt: »Die beiden Programme verletzten Bundesrecht sowohl im Wortlaut als auch im Geist. Es gibt kein Gesetz, dass massenhafte Überwachung ausdrücklich authorisiert.« In einer vollkommenen Welt würden wir schlichtweg rechtliche Mittel nutzen, um schlechte Gesetze auszulöschen und gravierende Ungerechtigkeiten zu bekämpfen. Kritiker sollten diesen Weg gehen, bevor sie das Gesetz brechen.

In diesem Fall ist genau das passiert. Seit Inkrafttreten des US PATRIOT Act, der während einer Zeit großer nationaler Angst und Zwang verabschiedet wurde, haben wir diverse Versuche von Bürgerrechtsorganisationen gesehen, die mit Rechtsmitteln die riesige Industrie des unbefugten Abhörens ohne richterlichen Beschluss einschränken wollten. Ein Gerichtsverfahren, das 2006 zuerst durch die Electronic Frontier Foundation und die American Civil Liberties Union gegen AT&T geführt wurde, wurde nicht nur hinausgezögert, sondern kam letztlich zum Erliegen. Grund dafür war ein dubioses Gesetz, das Telekommunikationsunternehmen, die mit der Regierung kooperierten, nachträglich Immunität gewährte. Das Gesetz wurde soweit gebogen bis es für diesen Fall nutzlos wurde.

Neben rechtlichen Anstrengungen haben Individuen auch versucht, andere zur Verfügung stehende Kanäle zu nutzen, um Veränderung herbeizuführen – jedoch ohne Erfolg. Wir müssen nur zu Thomas Drake blicken, dem langjährigen NSA-Mitarbeiter, der immer mehr Unbehagen aufgrund der Verstöße in seinem nächsten Umfeld verspürte. Er äußerte seine Bedenken gegenüber seinen Vorgesetzten und wurde aufgefordert, dies zu unterlassen. Er wandte sich mit geheimen Informationen an die Presse, wofür er teuer bezahlte. Das

Justizministerium ermittelte gegen ihn und erst als seine Karriere zerstört war, wurde das Verfahren eingestellt.

Die einzigen Taten, die eine substantielle Debatte und zarte Anzeichen von Änderung erzeugten, waren Snowdens Enthüllungen. Warum? Zuerst ist zu erwähnen, dass es keine sagenumwobene Mehrheit gibt, die Überwachung unterstützt. Als PRISM die ersten Schlagzeilen machte und Umfragen eingeholt wurden, waren lediglich 56% für staatliche Überwachung und die Umfragen erwähnten nicht, dass auch US-Amerikaner überwacht werden. Selbst dann, wie kann eine Zahl, die lediglich die Hälfte eines Landes verkörpert, als Mehrheit dargestellt werden? Sie kann es nicht. Dieses Problem ist noch lange nicht gelöst. Weiterhin haben sich die Zahlen verschoben als immer mehr Vorwürfe ans Tageslicht gelangten. Immer mehr Amerikaner sprechen sich gegen die aktuellen Programme aus, vor allem wenn die Fragen widerspiegeln, dass auch das digitale Leben von US-Amerikanern überwacht und abgespeichert wird.

Snowdens Gründe für das Veröffentlichen der Informationen können nicht einfach darauf reduziert werden, dass »Dinge nicht geheim gehalten werden sollten.« Seine Aussagen darüber, warum er getan hat was er getan hat und die Dokumente, die er enthüllt hat, zeigen eine wesentlich komplexere logische Grundlage, die wir bei unserer Analyse nicht auslassen dürfen. Was Snowden getan hat, war den Wasserhahn aufzudrehen, damit wertvolle Informationen der durstigen Öffentlichkeit zufließen können, die ein Recht auf dieses Wissen hat. Nur dann kann die Öffentlichkeit zu einer realistischen Einschätzung darüber kommen, wie sie weiter mit einer staatlichen Behörde verfahren will, die zur Zeit uneingeschränkte Macht zur Überwachung hat und die aktiv Informationen zurückgehalten und den Kongress über ihre Taten angelogen hat.

Manche mögen meine Rechtfertigung von Snowdens Taten kritisieren – durch Anfechtung der Annahme, dass die Öffentlichkeit ein »Recht auf Wissen« habe – jedoch zeigt schon ein seichtes Waten in das historische Becken der Verschwiegenheit der-US Regierung, dass dieses Argument nicht stichhaltig ist.

Die Geschichte hat gezeigt, dass Geheimhaltung, obwohl nötig, auch ein Nährboden für Missbrauch ist. In einer früheren Ära half eine dramatische Enthüllung durch die »Bürger-Kommission zur Untersuchung des FBI« einer 40-jährigen Herrschaft abscheulichen Missbrauchs ein Ende zu setzen – wie das »Counter Intelligence Program« (COINTELPRO), für das J. Edgar Hoover, der das FBI mit verschlossener eiserner Faust regierte, maßgeblich verantwortlich war.

Jedoch trumpft dieser heutige Überwachungsapparat als technologisch und somit historisch unvergleichlich auf. Es kann mit und ohne jemanden wie Hoover gravierend Missbrauch getrieben werden. Nie zuvor in der Geschichte hatten wir eine ähnlich weitreichende und mächtige Überwachungsinfrastruktur wie jetzt. Oder eine Regierung, die es so systematisch verweigert, Informationen zu veröffentlichen. (Man muss sich fragen, was Nixon und Hoover mit den Überwachungsmethoden getan hätten, die der Regierung heutzutage zur Verfügung stehen.) Mit genügend Rechenleistung ist es beängstigend einfach für die Regierung, Daten zu sammeln. Diese Einfachheit wird sie sehr wahrscheinlich dazu bringen, fragwürdige oder *ex post de facto* Rechtfertigungen für ihre Handlungen zu suchen. Dies wurde ziemlich stichhaltig und treffend durch Bürgerrechts-Anwältin Jennifer Granick ausgedrückt: »Natürlich sehen wir eine schleichende Ausweitung der Ziele – wenn man erst einmal die Mausefalle der Überwachungsinfrastruktur gebaut hat, werden sie kommen, um sich die Daten abzuholen.« Es geht nicht nur darum, dass sie die Möglichkeit haben; Soziologen und andere haben angemerkt, dass Geheimhaltung verführerisch und wirklich schwer aufzugeben ist. Diese Geisteshaltung wurde am besten durch den Physiker Edward Teller beschrieben: »Wenn man Geheimhaltung erst einmal eingeführt hat, wird sie zur Sucht.«

Es gibt vielleicht einen sehr guten Grund für die jetzigen Überwachungsmethoden der NSA, aber bis dieser Grund bekanntgegeben wird gibt es keinen Grund, dass sie solch wahnsinnige technische und (fragwürdige) rechtliche Macht besitzen, wie sie ihnen zur Zeit zur Verfügung steht. Das Problem ist, dass es diese Programme gibt und dass unsere Regierung sie als Werkzeug zur Unterdrückung

benutzen könnte (tatsächlich führt schon der simple Umstand ihrer Existenz zur Unterdrückung Andersdenkender). Selbst wenn es bisher keinen gravierenden Missbrauch gab, ist es besorgniserregend, dass diese Programme es jeder zukünftigen Person, der sie in die Hände fallen, ermöglichen, sie zu schwerwiegender Unterdrückung zu benutzen.

Als Gesellschaft müssen wir uns fragen, ob wir bereit sind, dieses Spiel mitzuspielen. Da für die Zukunft so viel auf dem Spiel steht, kann und sollte die Entscheidung über Umfang und Tiefe des Abhörens nicht beim Präsidenten, dem FISA Gericht oder sogar einvernehmlich bei allen drei Zweigen der Regierung liegen. Einzig wir als das Volk, die die in der Verfassung festgeschriebenen Wahrheiten als selbstverständlich annehmen, sind von ebenjener Verfassung dazu berechtigt, solche fundamentalen Rechte zu verändern. »Um diese Rechte zu sichern, wurden Regierungen für die Menschen eingerichtet, die ihre Macht aus der Zustimmung der Regierten beziehen, – und wenn dieses Ziel nicht befolgt wird, ist es das Recht des Volkes, diese zu verändern oder abzusetzen und eine neue Regierung zu bilden« An einem bestimmten Punkt führen die Handlungen der Regierung zu weit und es ist unsere Aufgabe, die Alarmglocken zu läuten. Die Pentagonberichte, die COINTELPRO-Leaks, die Tet-Offensive, es gibt viele Beispiele dafür, dass die Bürger unseren gewählten Vertretern aus gutem Grund misstraut haben.

Es ist unsere Verantwortung, unsere gewählten Abgeordneten zur Rechenschaft zu ziehen, obgleich wir dies effektiv nur mithilfe einer freien Presse können. Journalisten helfen, Whistleblower glaubwürdig zu machen. Snowden arbeitete mit Journalisten, von der unabhängigen Filmemacherin Laura Poitras über Glenn Greenwald vom Guardian bis zu Barton Gellman bei der Washington Post. Die Tatsache, dass angesehene Nachrichtenagenturen die Enthüllungen akzeptierten, Informationen filterten und umfangreiche und tiefgründige Artikel darüber schrieben, verdeutlicht die Validität und das Verantwortungsbewusstsein von Snowdens Taten. Ich vertraue darauf, dass diese Medieneinrichtungen die Leaks nicht veröffentlicht hätten,

falls seine Enthüllungen eine derart ernsthafte Gefahr für die Sicherheit des Staates darstellen würden.

Zum Abschluss möchte ich gerne Snowdens Aussagen bzgl. Nürnberg erläutern. Er setzt die NSA nicht mit dem Dritten Reich gleich, er stellt ganz einfach Bezüge zu den Prinzipien her. Weiterhin sagt er nicht, dass diese ihn vor irgendeinem US-amerikanischen Gericht entlasten, sondern lediglich, dass sie seine Taten auf moralischer Ebene rechtfertigen. Snowden sagt, dass es Zeiten gibt, in denen es nicht nur moralisch richtig ist, das Gesetz zu brechen, sondern dass es unmoralisch und falsch ist, das Gesetz nicht zu brechen. Weiterhin könnte es interessant sein, sich auf das Gedankenexperiment darüber einzulassen, wie Snowdens Taten in Beziehung zu den Nürnberger Prinzipien stehen. Für den Zweck dieses Experiments würden wir einige unbestreitbare Fakten über die USA vorlegen. Die USA foltern und quälen fortwährend Menschen, die immer noch gegen ihren Willen in Guantanamo Bay auf Kuba festgehalten werden. Dies geschieht durch nasale Intubation, die zweimal täglich erfolgt. In der Vergangenheit wurden sie durch Elektroschocks an den Genitalien und simuliertem Ertrinken durch Waterboarding gefoltert. Die Vereinigten Staaten haben Menschen gewaltsam an andere Staaten übergeben, damit diese dort gefoltert werden können und haben ihnen somit ihre Freiheit ohne Anklage oder ein ordentliches Verfahren aberkannt. Die USA nennt sie »ungesetzliche Kombattanten«. Wenn wir uns ansehen, wie die Nürnberger Prinzipien ein »Verbrechen gegen die Menschheit« definieren, haben sich die USA über der Hälfte der Verbrechen auf dieser Liste schuldig gemacht. Die Programme, die durch Snowden enthüllt wurden, waren wahrscheinlich beim Erfassen und Wegsperren einiger dieser Menschen involviert. Eine Geschichte an Missbräuchen, sowohl gegenwärtig als auch in der Vergangenheit, liefert wenig Gründe um sicher zu sein, dass mit der vorhandenen Überwachungsinfrastruktur verantwortungsbewusst umgegangen würde.

Wenn so viele unterschiedliche Positionen innerhalb der Gesellschaft dem vorherrschenden Rechtssystem nicht länger vertrauen können, ein Wächter über die Überdehnung staatlicher Überwachung zu sein,

müssen wir auf die Freiheit der Presse und Medieneinrichtungen vertrauen. Zeit ist ausschlaggebend, wenn es um das Recht der Öffentlichkeit geht, aufgeklärt zu werden. Je länger die Öffentlichkeit nichts vom unrechtmäßigen Wachstum der Ranken namens »Sicherheit« weiß, desto stärker und umfassender werden diese gedeihen.

Vor diesem Post-9/11-Hintergrund ist es entscheidend, die Verbindungen zwischen den von Snowden enthüllten Programmen, der Rolle der Medien bei deren Veröffentlichung und ihren Auswirkungen auf das Vorantreiben der Menschenrechtsverstöße durch die USA zu bedenken. Vor allem das Erfassen und Wegsperren vermeintlich »Krimineller« ohne Anklage oder ordentliches Verfahren in Guantanamo Bay, Kuba. Es geht nicht einfach um das derzeitige Nutzen und den Missbrauch von Überwachungstechnologie (obgleich es hinreichend belegte Beweise über den Missbrauch dieser Macht gibt), sondern genauso um das heikle Potenzial zukünftigen Missbrauchs und das damit einhergehende Verstummen von Widerspruch und Veränderung.

Letztlich möchte ich, wie jeder andere auch, in Sicherheit leben. Das bedeutet nicht nur die Abwehr von Terrorismus – allerdings schließt es dies ausnahmslos mit ein – sondern bedeutet auch, die Sicherheit zu haben, widersprechen zu dürfen. Die Sicherheit, auf die ernsthaften Menschenrechtsverstöße – wie die in Guantanamo Bay – hinzuweisen, die durch unsere gewählten Vertreter immer noch andauern. Und vor Programmen wie PRISM zu warnen, die zu erheblichem zukünftigen Missbrauch führen könnten.

Die Art von leidenschaftlicher Debatte, die durch Snowden angeregt wurde und das eifrige Entstehen von Koalitionen und Befürwortern, das als Folge dieser Enthüllungen spontan aufkam, und gerade nicht das blinde Vertrauen in dubiose Gesetze, verkörpern den Pulsschlag der Demokratie. Wir stehen in Snowdens Schuld, dass er uns die Tore geöffnet hat. Es liegt nun an uns, die Aufgabe zu beenden.

Dieser Text ist zuerst am 23. August 2013 im Blog der Princeton University Press erschienen[72] *und wurde für dieses Buch ins Deutsche übersetzt.*

Die europäische Datenschutzreform zu missachten, ist ignorant

Benjamin Bergemann

»Die schöne neue Welt der NSA ist nichts anderes als Wal Mart plus staatliches Gewaltmonopol minus politische Kontrolle«, schreibt Frank Schirrmacher in einem der weitsichtigsten Essays nach den Enthüllungen Edward Snowdens[73]. Sowohl die NSA als auch Wal Mart existieren, weil sie Daten lesbar machen und verwerten. Diese Datensätze sind wir. Snowden hat uns begreifen lassen, dass wir in einer Informationsgesellschaft leben. So gewiss diese Erkenntnis scheint, so umstritten ist, welche Konsequenzen wir daraus ziehen.

Viele Menschen sehen lediglich im unkontrollierten staatlichen Gewaltmonopol ein Problem. Nachrichtendienste sollten nicht ungehindert auf die Daten von Unternehmen zugreifen. Da Datenschutzgesetze dieses Problem nicht unmittelbar lösen, sind sie für diese Menschen wenig relevant.

Besonders hart trifft diese Sicht die Datenschutzgrundverordnung, die derzeit auf europäischer Ebene verhandelt wird. Die Datenschutzreform geriet kurz als Exempel für die Auswüchse des Brüsseler Lobbyapparates in die Schlagzeilen[74]. Wenige Wochen vor der entscheidenden Abstimmung im Europäischen Parlament gibt es kaum noch öffentliche Aufmerksamkeit für das Gesetzesvorhaben[75]. Immerhin wird die Verordnung den europäischen Datenschutz der nächsten Jahrzehnte regeln. Sich ausgerechnet jetzt nicht für dieses Gesetz zu interessieren, ist ignorant.

Denn *erstens* gibt es kaum Anzeichen dafür, dass die Nachrichtendienste von nun an effektiv kontrolliert würden. Ihre undemokratische Struktur entzieht sich systematisch der Kontrolle. Das gilt besonders, wenn es sich um derart gewachsene Systeme handelt, wie Snowden sie der Welt

offenbart hat[76]. Folgendes simple Prinzip ist daher zumindest in Betracht zu ziehen: Daten, die nicht erhoben werden oder technisch nicht ohne weiteres zugänglich sind, machen es den Nachrichtendiensten erheblich schwerer. Wohlgemerkt handelt es sich dabei nicht um die Lösung des Problems, sondern um eine sinnvolle Maßnahme unter vielen.

Zweitens ist es nicht so, dass Daten allein in staatlichen Händen Missbrauchspotenzial bergen. Wie ihr Vorgänger im 19. Jahrhundert, verändert auch die »zweite industrielle Revolution« (Schirrmacher) unsere gesamte Lebens- und Arbeitswelt. Wie damals sind es nicht die Schwächsten, die profitieren – im Gegenteil. Die Tagelöhner heißen heute Risikogruppen. Unternehmen, Banken, Versicherungen und auch öffentliche Behörden treffen Entscheidungen über Menschen zunehmend datenbasiert.

In Anbetracht dieser Tatsachen erscheint die Datenschutzverordnung als lohnendes Projekt. Sie kann dabei helfen, Datenströme zwischen uns, Unternehmen und Behörden zu *regulieren*, wenn sie das Prinzip der Zweckbindung der erhobenen Daten zukunftssicher festschreibt[77]. Das »legitime Interesse«, eine Rechtsgrundlage der Datenverarbeitung ohne Zustimmung der Betroffenen, sollte zumindest auf konkrete Fälle eingeschränkt werden[78]. Diese Maßnahmen verlangen besonders im Hinblick auf die Datenweitergabe an Dritte Beachtung.

Die Datenschutzverordnung kann nicht vor nachrichtendienstlichem Zugriff auf Daten schützen – vor allem nicht wenn diese in den USA liegen[79]. Auch kann und soll sie die Einwilligung in datenintensive Dienste nicht verhindern. Dafür kann sie durch Transparenzverpflichtungen (z.B. in Symbolform[80]) dazu beitragen, ein *Bewusstsein* bei den Nutzer/innen zu schaffen. Worin willige ich da eigentlich ein und welche Daten von mir werden wie verarbeitet? Dazu gehört auch ein uneingeschränktes Recht auf Auskunft und Löschung personenbezogener Daten.

Diese Dinge bleiben ohne *Kontrolle und Durchsetzung* wertlos. Das ist auch das Schicksal der derzeit geltenden europäischen Datenschutzrichtlinie. Es braucht einen handlungsfähigen europäischen Datenschutzausschuss sowie gut ausgestattete nationale Datenschutzbehörden. Diese sollten zudem Vorgaben zum technischen Datenschutz festsetzen und an ihrer Entwicklung mitwirken.

Von der »zweiten industriellen Revolution« müssen so viele Menschen wie möglich profitieren. Die Datenschutzverordnung ist ein Baustein dazu. Richtig umgesetzt kann sie dazu beitragen, dass technischer Fortschritt und Datenschutz kein Widerspruch sein müssen. Sie streift allerdings auch viele Probleme, die umfassender an anderer Stelle behandelt werden müssen: Wie einigen wir uns auf Datenschutzregeln außerhalb Europas? Instrumente wie das Safe Harbor-Abkommen zum Datentransfer in die USA sind obsolet[81]. Wie schützen wir Whistleblower wie Edward Snowden? Dass wir von europäischen Missständen erst durch ihn erfahren haben, spricht für sich. Wie viel Nachrichtendienst dürfen Polizeibehörden sein? Auch hier beobachten wir den Paradigmenwechsel hin zu präventiver Datensammlung und -auswertung. Quer dazu liegt die Frage, wie die »Gesellschaftssoftware« Internet in Zukunft aussieht: Große goldene Käfige und proprietäre Standards oder dezentrale Strukturen auf Open-Source-Basis?

Der abschreckende Effekt von Überwachung

Infragestellung der Vorstellung, wir hätten dem Staat gegenüber »nichts zu verbergen«

Jillian York

Die Enthüllungen, die in den Dokumenten enthalten waren, die im Sommer 2013 von Edward Snowden geleakt wurden, haben die Vereinigten Staaten an die Spitze der fortwährenden globalen Debatte um Überwachung gesetzt. Die Orwellsche Geschichte, die mit dem Bericht über die Zusammenarbeit des Telekommunikations-Anbieters Verizon mit der NSA begann, erschließt sich immer weiter und jede Enthüllung scheint schwerwiegender als die vorangegangene. In ihrer Gesamtheit wirkt die ganze Geschichte wie ein Roman aus der Zukunft.

Betrachte für einen Moment den Tribut konstanter Überwachung auf das Wohlergehen von Bürgern in der Sowjetunion oder Ostdeutschland. Forschungen über die Effekte solch tiefgreifenden Ausspionierens haben gezeigt, dass ihre Subjekte befangen und ängstlich werden. Der Langzeitschaden zeigt sich auf unterschiedlichste Arten, die abschreckendste ist vielleicht das Entstehen einer Kultur der Selbstzensur.

Während sich in solchen Regimen die Impulsgeber der Spionage gerne bedeckt gaben, argumentieren heute die Befürworter der Überwachung ganz offen – gerne unter dem Deckmantel der inneren Sicherheit. Elektronisches Spionieren sei notwendig, um Terroristen zu fangen, sagen sie. Die heutige schleppnetzartige Überwachung ist kein bisschen weniger schädlich als die vergangener Tage, auch wenn sie anders angelegt ist: Statt sich auf Dissidenten und ähnliche Ziele zu fokussieren, werden heute im Namen des Staatsschutzes Telefon- und Onlinekommunikations-Metadaten von Millionen von Menschen gesammelt.

Außerhalb der Vereinigten Staaten ist der Widerstand gegen die NSA-Überwachung klar und deutlich. In Brasilien sollen Daten innerhalb der

Staatsgrenzen gebunden werden. In Deutschland wird die Regierung unter Druck gesetzt, den nachrichtendienstlichen Datentausch mit den USA einzustellen. In Indien verwenden Aktivisten den Schaden, der durch die NSA-Spionage entstanden ist, als Argument gegen die Überwachungsmaßnahmen der eigenen Regierung. Die Beispiele mehren sich.

Aber in den USA wird eine andere Geschichte erzählt. Dort stehen sich diejenigen gegenüber, die von sich behaupten »nichts zu verbergen« zu haben, und diejenigen, die den sich abzeichnenden Schaden eines solchen großflächigen Spionage-Programms erkennen.

Diejenigen, die das erste Argument verwenden, tun das aufgrund eines tief verwurzelten Vertrauens in die US-Regierung. Die Annahme scheint zu sein, dass Überwachung notwendig ist, um die USA gegen Terrorismus zu schützen, obwohl es für die Wirksamkeit wenig Beweise gibt. Eine weitere, oft geäußerte Überzeugung ist, dass Massenüberwachung an sich zwar ein Problem darstellt, den USA aber vertraut werden kann, da sie ihr Augenmerk nur auf die »bösen Jungs« richteten.

Das ist offenkundig falsch. Im letzten Jahrzehnt wurden zahlreiche Machtmissbräuche von US-Behörden bekannt, von der Beobachtung von Aktivisten, die sich für Solidarität mit Palästina einsetzten, über die Verfolgung von WikiLeaks bis hin zur Infiltrierung und dem Ausspionieren muslimischer Gemeinschaften. Das Argument, dass das US-System nicht missbraucht werden kann oder wird, ist schlichtweg hinfällig.

Die Verfolgung von Whistleblowern unter der Regierung von Obama zeigt außerdem, dass die US-Regierung eventuell nicht derart wohltätig ist, wie sie sich darstellt. Die kürzlichen Anschuldigungen gegen Snowden machen ihn zum achten Leaker, der während Obamas Amtszeit unter dem Espionage Act angeklagt wurde; vor seiner Amtseinführung wurde dieser nur zur Verfolgung *dreier* Einzelpersonen herangezogen, einschließlich Daniel Ellsberg.

Nichtsdestotrotz werden einige vorbringen, dass Überwachung zwar eine Last ist, aber weitaus weniger bedeutend als andere soziale Missstände wie Armut oder Gesundheitsvorsorge in den USA. Ohne die Freiheit, solche Bedürfnisse anzusprechen, werden auch alle anderen Bemühungen schwieriger.

Als Sonderberichterstatter der UN für freie Meinungsäußerung schrieb Frank LaRue vor Kurzem, »Ungeachtet dessen, dass ein Eingriff in die Privatsphäre sowohl direkt als auch indirekt die freie Entfaltung und den Austausch von Ideen einschränken kann, [...] kann ein Verstoß gegen ein Recht sowohl Grund als auch Konsequenz eines Verstoßes gegen ein anderes darstellen.« Ohne Redefreiheit sind alle Formen von Aktivismus oder das Infragestellen staatlicher Befugnisse bedroht. Und um sich greifende Überwachung bedroht ganz deutlich unsere Fähigkeit, frei zu sprechen, indem sie ein Klima der Angst erzeugt.

Dieser Text wurde von der Redaktion ins Deutsche übersetzt.

Welche Konsequenzen haben PRISM und Tempora für den Datenschutz in Deutschland und Europa?

Peter Schaar

Was waren das noch für schöne Zeiten, als man das Internet nutzen konnte, ohne sich über Registrierung, Profilbildung und Überwachung Gedanken zu machen! Diese Zeiten liegen lange zurück. Spätestens seit den Veröffentlichungen der internationalen Presse aus Papieren, die der ehemalige Geheimdienstmitarbeiter Edward Snowden »mitgenommen« hat, müssen wir uns dran gewöhnen, dass es kein Zurück in den Zustand der Unschuld gibt.

Die staatliche Überwachung betrifft nicht mehr vorwiegend Personen, die krimineller oder terroristischer Handlungen verdächtig sind. Sie betrifft jeden, der das Internet nutzt, und sie ist global angelegt. Die für die umfassende Überwachung Verantwortlichen in Politik und Behörden unterlaufen so die durch die Verfassungen in aller Welt verbürgten Garantien. Das US-Programm PRISM und das britische System Tempora stehen für einen Ansatz, der letztlich alles wissen will, nach einem dem ehemaligen DDR-Staatssicherheitsminister Erich Mielke zugeschriebenen Motto: *Um wirklich sicher zu sein, muss man alles wissen.*

Historischer Hintergrund

Viele Fakten, die jetzt aufgeregt diskutiert werden, sind seit langem bekannt. Seit dem Ersten Weltkrieg überwachte eine beim US-Verteidigungsministerium assoziierte Behörde (*Black Chamber*) den Brief- und Telegraphenverkehr der Botschaften in der US-Hauptstadt. Dieses schwarze Kabinett war der Vorläufer der heutigen *National Security Agency* (NSA). So lange zurück reichen auch die engen Beziehungen zwischen dieser Behörde und den Telekommunikationsunternehmen.

Die Depeschen der diplomatischen Vertretungen wurden – ohne gesetzliche Grundlage – über die Schreibtische der Spionageorganisation umgeleitet, dort kopiert und – soweit die Nachrichten verschlüsselt waren – nach Möglichkeit dekodiert. Darüber berichtet etwa *David Kahn* in seinem 1967 erschienenen Werk *The Codebreakers*.

Auch der Beginn des Computerzeitalters ist aufs Engste mit Geheimdiensten verbunden. Sogar das Konzept des modernen Universalcomputers, auf dem praktisch alle heutigen Systeme basieren, verdanken wir den Codebreakers im britischen Bletchley Park, allen voran dem hier tätigen Mathematiker Alan Turing. Ihnen gelang während des Zweiten Weltkriegs gar die Entschlüsselung des vom deutschen Militär eingesetzten Chiffriersystems ENIGMA.

Nach dem Zweiten Weltkrieg wurden die Horcher und Lauscher weiterhin benötigt, jetzt allerdings für den Kalten Krieg zwischen den »Westmächten« und dem »Ostblock«. Die NSA wurde 1952 auf Anweisung des US-Präsidenten unter absoluter Geheimhaltung gegründet. Selbst ihre bloße Existenz wurde geheim gehalten und wurde erst 1957 eher beiläufig bekannt gegeben – hartnäckig hält sich deshalb bis heute der Scherz, NSA stehe für *No Such Agency*.

Stets ging es der NSA darum, sich ein möglichst umfassendes Bild von der weltweiten Kommunikation zu verschaffen. Dabei kooperierte man vornehmlich mit den anderen Mitgliedern des exklusiven *Five Eyes*-Clubs – außer den USA gehören dazu die Nachrichtendienste Großbritanniens, Kanadas, Australiens und Neuseelands. Bekannt geworden sind deren Aktivitäten in den 1990er Jahren zunächst unter dem Stichwort Echelon, einem System zur weltweiten Auswertung der Satellitenkommunikation.

1997 kam eine Studie, die im Auftrag des Europäischen Parlaments im Rahmen des *Scientific and Technological Options Assessment Programme* (STOA) erstellt worden war, zu dem Ergebnis, dass sämtliche Kommunikation via E-Mail, Telefon und Fax von der NSA routinemäßig überwacht werde – auch innerhalb Europas. Nach weiteren Studien hat das Europäische Parlament 2001 einen umfassenden Bericht

veröffentlicht, der zwar die Existenz von Echelon bestätigte, nicht aber alle ihm zugeschriebenen Eigenschaften, namentlich nicht die behauptete Totalüberwachung der Telekommunikation.

Zwar war Echelon zunächst gegen den »Ostblock« gerichtet. Allerdings wurde es auch nach dessen Auflösung 1990 weiter betrieben, offenbar auch unter Beteiligung weiterer Geheimdienste, etwa des deutschen Bundesnachrichtendienstes (BND).

Seit dem Aufbau von Echelon vor mehr als fünfzig Jahren hat sich die Welt der Telekommunikation allerdings drastisch verändert. Die Bedeutung der Satellitentechnik im Fernmeldeverkehr hat stark abgenommen. Der bei Weitem bedeutendste Teil der globalen Kommunikation wird heute über Glasfaserkabel abgewickelt. Zudem wurde die Telekommunikation digitalisiert. Praktisch die gesamte elektronische Kommunikation – auch der Telefonverkehr – wird heute über die durch das Internet bereitgestellte Infrastruktur abgewickelt. Insofern verwundert es nicht, dass die Energien der Überwacher sich in den letzten zwanzig Jahren verstärkt dem Internet zugewandt haben.

Vom Need to Know zum Need to Share

Die vornehmlich von Nachrichtendiensten verantworteten Aktivitäten hatten zunächst keinen erkennbaren Einfluss auf das in den 1970er und 1980er Jahren des 20. Jahrhunderts entwickelte Datenschutzrecht. Zu speziell erschienen die Bedingungen, unter denen Geheimdienste arbeiteten. Und nach der seinerzeitigen Wahrnehmung erschien es höchst unwahrscheinlich, dass der Einzelne zum Objekt geheimdienstlicher Informationsbeschaffung wurde. Heute wissen wir es besser!

Das in den 1970er Jahren formulierte Datenschutzrecht war eine Reaktion auf Gefahren der automatisierten Datenverarbeitung. Sein Hauptanliegen besteht darin, die Verarbeitung personenbezogener Daten zu begrenzen und deren Verwendung zu steuern. Von Beginn an ging es dabei um einen Interessenausgleich zwischen den Betroffenen und den Nutznießern der Verarbeitung, seien diese staatliche oder privatwirtschaftliche Akteure.

Zwei lange Zeit unbestrittene datenschutzrechtliche Schlüsselkonzepte sind die der Datensparsamkeit und Erforderlichkeit: Jede Stelle, die personenbezogene Daten sammelt, muss sich auf das zum Erreichen des angestrebten Ziels erforderliche Datenminimum beschränken. Für staatliche Stellen sind die Grundsätze der Erforderlichkeit Ausdruck des verfassungsrechtlichen Verhältnismäßigkeitsprinzips, wonach Grundrechtseingriffe sich auf das zur Aufgabenwahrnehmung notwendige Minimum zu beschränken haben.

Die Terroranschläge vom 11. September 2001 brachten jedoch auch für den Datenschutz eine Zäsur. Wenige Tage nach den Anschlägen erklärte US-Präsident George Bush den »Krieg gegen den Terror«. In seiner viel beachteten Rede am 20. September 2001 kündigte er an:

> *»We will direct every resource at our command – every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence, and every necessary weapon of war – to the destruction and to the defeat of the global terror network.«*[82]

Recht bald wurde klar, dass damit nicht nur ein militärisches Vorgehen gegen Afghanistan und andere Mitglieder der »Achse des Bösen« gemeint war, sondern auch ein erbarmungsloser Kampf gegen Gegner, die man bereits im eigenen Land vermutete, ein Kampf, der auch tiefe Einschnitte in Bürgerrechte in Kauf nahm.

Der *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (US PATRIOT Act) räumte den Geheimdiensten und dem *Federal Bureau of Investigation* (FBI) sehr weitgehende neue Befugnisse ein. Die beschlossenen Maßnahmen umfassen Vollmachten zum Abhören von Telefonen, zum Mitlesen von E-Mails und zum geheimen Zugriff auf alle möglichen privaten Datenbestände, von durch Telefongesellschaften gespeicherten Telekommunikationsdaten bis hin zu Dateien über das Leseverhalten in öffentlichen Bibliotheken.

Vor allem amerikanische Sicherheitsbehörden sahen in den, durch das Datenschutzrecht vorgegebenen, Regeln unzeitgemäße Behinderungen im »Krieg gegen den Terror«. Die US-Administration folgte nach den terroristischen Anschlägen dem Credo, immer mehr Daten aus unterschiedlichsten Quellen zusammenzuführen: *Need to Know*, damit wurde der Erforderlichkeitsgrundsatz von gestern. Im »Krieg gegen den Terror« müssten auch alle möglichen, aus den unterschiedlichsten Quellen stammenden Informationen zusammengeführt werden, gemäß der neuen Maxime: *Need to Share*. Eventuell ließen sich so Verhaltensmuster erkennen und Terroranschläge verhindern.

Auch wenn die Umsetzung des US PATRIOT Act von der US-Administration weitgehend als Geheimangelegenheit behandelt wurde, sickern immer wieder beunruhigende Einzelheiten an die Öffentlichkeit. So wurde 2006 bekannt, dass die NSA entgegen dem damaligen Wortlaut des *Foreign Intelligence Surveillance Act* (FISA) viele Millionen Daten über die Telekommunikation (sogenannte Metadaten) ohne richterliche Anordnung von Telefonunternehmen angefordert und erhalten hatte, und zwar auch solche Daten, die ganz überwiegend US-Bürger betrafen. Nach Presseberichten war zudem praktisch jedes Auslandstelefonat Gegenstand des NSA-Überwachungsprogramms. Die Konsequenz aus dieser Berichterstattung bestand allerdings nicht in der Beschränkung der Überwachung. Vielmehr wurden die aufgedeckten Praktiken mit dem *FISA Amendments Act of 2008* nachträglich im Wesentlichen legalisiert. Die an den illegalen Überwachungsaktionen Beteiligten wurden so straffrei gestellt.

Die Überwachung des Internets

In dem 2008 von *James Bamford* veröffentlichten Werk *The Shadow Factory* ist nachzulesen, wie die NSA das Internet mit Überwachungstechnik überzogen hat. Die dabei entwickelten Überwachungsinstrumente ermöglichen das Erfassen, Mitschneiden und Auswerten der Kommunikation, und zwar sowohl der Meta- als auch der Inhaltsdaten. Schon seit 1994 verpflichtet ein US-Gesetz namens *Communications Assistance for Law Enforcement Act* (CALEA) die

Telekommunikationsunternehmen, ihre Systeme so zu gestalten, dass sie einfach zu überwachen sind.

Den Überwachern kommt dabei entgegen, dass die zentralen Internet-Vermittlungseinrichtungen überwiegend in den USA betrieben werden. So berichtete 2007 das Online-Magazin *Wired* über die Bedeutung der Struktur der Telekommunikationsnetze und des Internets für die Überwachungsaktivitäten der NSA.

Auch wenn es keine Belege für die These gibt, dass die Steuerung der Datenströme (sogenanntes Routing) über US-Knoten durch bewusste Intervention von Geheimdiensten herbeigeführt wurde, gehören die Lauscher doch zu den Profiteuren. *James Bamford* beschreibt detailliert, wie die NSA die dominante Rolle der USA in der globalen Kommunikation zur umfassenden Überwachung nutzt, etwa bei der Ausleitung und Überwachung von Unterseekabeln an ihren Landestationen an der US-Küste oder zur Überwachung des jetzt zu einiger Berühmtheit gekommenen Transatlantik-Glasfaserkabels TAT-14.

Bestätigt wird dies auch durch eine von Edward Snowden geleakte und durch die *Washington Post* veröffentlichte Präsentation über das Programm *Planning Tool for Resource Integration, Synchronization, and Management* (PRISM), in der darauf hingewiesen wird, dass ein Großteil der weltweiten Kommunikation über die USA geleitet wird (*U.S. as World's Telecommunications Backbone*).

PRISM

Die Veröffentlichungen der *Washington Post*, des *The Guardian* und der *The New York Times* seit dem 6. Juni 2013 haben eine weitere besonders kritische Seite der Überwachung verdeutlicht: Nicht bloß die laufende Kommunikation wird überwacht. Darüber hinaus »kooperieren« die größten Internet-Unternehmen von Google über Yahoo bis Microsoft und Facebook angeblich mit den Überwachern aus der NSA.

Einen Tag nach der Veröffentlichung, am 6. Juni 2013, gaben verschiedene in den Unterlagen genannte Firmen praktisch gleich

lautende »Dementis« heraus, bei denen es sich lohnt, die Wortwahl etwas genauer zu betrachten. So liest man etwa im offiziellen *GoogleBlog*:

> *»First, we have not joined any program that would give the U.S. government—or any other government—direct access to our servers. Indeed, the U.S. government does not have direct access or a »back door« to the information stored in our data centers. [...] Second, we provide user data to governments only in accordance with the law. [...] Press reports that suggest that Google is providing open-ended access to our users' data are false [...].«* [83]

Interessant sind dabei insbesondere die folgenden Aussagen:

- Es gäbe keinen direkten Zugang zu unseren Servern.
- Was ist mit einem »indirekten Zugang«, etwa über Server, die der NSA gehören?
- Kann die NSA auf Netzkomponenten zugreifen, etwa auf Router, über die die für Google bestimmten Daten laufen?
- Benutzerdaten würden nur in Übereinstimmung mit dem Gesetz zur Verfügung gestellt.
- Metadaten müssen nach US-Recht herausgegeben werden, wenn allgemeine Gründe vorliegen, etwa dass Terroristen entsprechende Dienste nutzen (können). Individualisierter Anordnungen bedarf es nicht.
- Die gesetzlichen Bestimmungen schützen die Inhaltsdaten ausländischer Nutzerinnen und Nutzer weitaus weniger als diejenigen von US-Bürgern.

Inzwischen deklassifizierte Dokumente belegen, dass sich die Überwachung nicht nur gezielt gegen einzelne Personen richtet. So wurden Telekommunikationsunternehmen verpflichtet, sämtliche Metadaten ihrer Kunden an die NSA zu übermitteln. Die entsprechenden Anordnungen wurden stets kurz vor Ablauf erneuert; die Daten blieben gespeichert.

Die NSA hat an den zentralen, in den USA gelegenen, Internetknoten Zugang zu den dort durchlaufenden Datenströmen und zeichnet zumindest die Metadaten auf. Ferner greift der britische Nachrichtendienst *UK Government Communications Headquarters* (GCHQ) in großem Umfang Daten ab, die über Transatlantik-Leitungen laufen und übermittelt sie an die NSA.

Die Behauptung Googles, es gäbe keine Hintertüren zu den Daten, die in den Google-Rechenzentren gespeichert werden, erscheint zunächst plausibel. Allerdings verpflichtet CALEA nicht nur Telekommunikationsunternehmen zur Bereitstellung von Schnittstellen zur Ausleitung der Kommunikationsdaten. US-Telekommunikationsunternehmen dürfen nur solche Techniken verwenden, die mit entsprechenden Schnittstellen ausgestattet sind. Dies betrifft auch Internetrouter.

So berichtete die Presse wiederholt und detailgenau darüber, dass Router US-amerikanischer Hersteller mit entsprechenden Hintertüren ausgestattet sind. Es stellt sich also die Frage, inwieweit auch Google und andere Internetunternehmen entsprechende Technik einsetzen und ob sie wirklich verhindern können, dass darüber ein unautorisierter Zugriff stattfindet.

Im übrigen hat das FBI bestätigt, dass die amerikanische Regierung eine Ergänzung von CALEA anstrebt, durch die die Internetunternehmen unter Androhung hoher Strafzahlungen zur Einrichtung eines direkten Zugriffs der Sicherheitsbehörden auf die eigenen Server verpflichtet werden sollen. Ob diese Pläne auch nach den Snowden-Veröffentlichungen weiterverfolgt werden, bleibt abzuwarten.

Die internationale Presse hat nach und nach weitere Informationen aus dem PRISM-Fundus veröffentlicht. Besonders beunruhigend sind Berichte über die Aktivitäten der NSA und des britischen Geheimdienstes zur Schwächung und Kompromittierung von Sicherheitsmechanismen, insbesondere der Datensverschlüsselung und zur Gewährleistung der anonymen Nutzung des Internets.

Nach den Unterlagen soll dieses Unterfangen auf verschiedenen Ebenen gelungen sein: Neben *Brute Force* also dem Brechen von Schlüsseln durch Einsatz besonders leistungsfähiger Computer, sei es gelungen, die Mechanismen zur Schlüssel- und Zertifikatserzeugung zu manipulieren, etwa indem der Adressraum von hierbei verwendeten Zufallszahlengeneratoren künstlich eingeschränkt worden sei.

Sogar bei der Standardisierung sei es gelungen, Schwachstellen einzubauen, die zur Überwachung genutzt werden können. Damit sei es möglich, auch die verschlüsselte Datenkommunikation weiterhin mitzulesen und inhaltlich auszuwerten.

Auch das Anonymisierungsnetzwerk Tor sei Gegenstand erfolgreicher Manipulationsaktivitäten gewesen, mit denen es gelungen sei, die Identität der Tor-Nutzer herauszufinden.

Sind wir betroffen?

Sofern deutsche und andere europäische Bürgerinnen und Bürger einen US-Diensteanbieter nutzen, dessen Datenverarbeitung in den USA erfolgt, ist davon auszugehen, dass ein entsprechender Zugriff der US-Sicherheitsbehörden unter den Voraussetzungen der dortigen sehr weitgehenden Vorschriften (insbesondere US PATRIOT Act und FISA) erfolgt. Dies gilt im Prinzip auch für Server und Dienste, etwa Cloud-Services, die von US-Unternehmen außerhalb der USA, etwa in Europa, betrieben werden. Die US-Überwachungsanordnungen verpflichten diese Unternehmen unabhängig vom Ort der Datenverarbeitung.

Aber selbst derjenige Nutzer, der US-Dienste meidet, kann betroffen sein. Schließlich kooperieren viele Internetunternehmen mit Werbe- und Reichweitenmessdiensten, die aus den USA gesteuert werden. Auf diese Weise gelangen Nutzungsdaten auch auf deren Server.

Schließlich ist das Routing im Internet, also die Wegewahl der Datenpakete, im Regelfall so gestaltet, dass nicht ausgeschlossen werden kann, dass eine inländische etwa von Hamburg nach Berlin gesandte Mail nur über Datenleitungen und Router im Inland geht – sie kann auch den Umweg über einen US-Router nehmen.

Konsequenzen für den Datenschutz und das Fernmeldegeheimnis

Wie anfangs gesagt: Es gibt kein Zurück ins Stadium der Unschuld. Aber trotzdem gibt es politische, rechtliche und technologische Stellschrauben, die einer näheren Betrachtung bedürfen:

- Wir brauchen Klarheit über den Umfang der Überwachung! Die US-Behörden und die mit ihnen kooperierenden Unternehmen müssen alle Zahlen und Fakten auf den Tisch legen! Auch die Regierungen der europäischen Staaten – darunter Deutschland – müssen für Transparenz der eigenen Überwachungsprogramme sorgen. Die Bundesregierung hat die Affäre völlig zu Unrecht für beendet erklärt.

- Transparenz ist auch hinsichtlich der gegenseitigen Datenübermittlung erforderlich! Welche Daten werden welchen ausländischen Behörden zur Verfügung gestellt? Auf welcher Rechtsgrundlage geschieht dies? Und für welche Zwecke werden diese Daten von den Empfängern verwendet?

- Die Differenzierung des Schutzniveaus zwischen In- und Ausland, zwischen eigenen Staatsangehörigen und Ausländern, ist heute nicht mehr zeitgemäß. Die Befugnisse zur staatlichen Überwachung müssen durch nationales, europäisches und internationales Recht begrenzt werden! Die Bundesregierung und die Europäische Union sollten sich für ein internationales Übereinkommen zum Datenschutz einsetzen, das auch die staatliche Überwachung umfasst.

- Die in vielen internationalen Verträgen zu findenden Ausnahmen, die den betroffenen Staaten nahezu unbegrenzte Möglichkeiten geben, für Zwecke der »nationalen Sicherheit« abzuweichen, sind nicht mehr zeitgemäß und machen die Vereinbarungen zu Makulatur. Das gilt etwa für das *Safe Harbor*-Abkommen, auf dessen Basis viele US-Unternehmen Daten aus Europa erhalten und in den USA verarbeiten. Da diese Daten gegenüber US-Behörden nicht wirklich geschützt sind, kann hier von einem

»angemessenen Datenschutzniveau« nicht die Rede sein. Dies muss auch bei der aktuell diskutierten Reform des europäischen Datenschutzrechts berücksichtigt werden.

- Selbst wenn es gelingt, die Überwachungsaktivitäten westlicher Geheimdienste durch rechtliche Vorgaben zurückzuschneiden, was ich für durchaus zweifelhaft halte, ist damit überhaupt nicht gesagt, dass sich Nachrichtendienste anderer Staaten dadurch beeindrucken lassen. Deshalb müssen Datenschutz und Fernmeldegeheimnis technologisch flankiert werden. Die Technik ist so zu gestalten, dass die Grundsätze der Erforderlichkeit, Zweckbindung und Vertraulichkeit gewährleistet werden.

- Die Datenverschlüsselung ist nach wie vor von zentraler Bedeutung für den Schutz vertraulicher Daten, auch wenn man Kryptoverfahren nicht blind vertrauen kann. Neben den Kryptoalgorithmen muss dabei besonderes Augenmerk auf das technische Umfeld ihres Einsatzes, auf Hard- und Software gelegt werden. Nur so lassen sich Hintertüren und Schwachstellen vermeiden. Die Ende-zu-Ende-Verschlüsselung, durch die die Inhalte wirksam geschützt werden können, und die Verschlüsselung von Verbindungen – zum Schutz der Metadaten – können sich dabei ergänzen.

- Zwar ist es nicht sinnvoll, das Internet in kleine nationale Parzellen zu unterteilen. Gleichwohl sollte durch technische Mittel darauf hingewirkt werden, dass rechtliche Garantien nicht durch die Wegewahl von Datenpaketen unterlaufen werden. So sollte beim Routing das Prinzip des kürzesten Wegs gelten. Die (Um-)Leitung von Datenpaketen über Staaten mit unzureichendem Datenschutz sollte möglichst vermieden werden.

Aufklärung à la EU

Alexander Sander

Als der Guardian am 5. Juni die ersten Informationen über die gigantische Überwachung aller Bürger/innen durch amerikanische Geheimdienste publik machte[84] war die Reaktion in der EU verhalten. Nur einzelne Abgeordnete des EU-Parlaments veröffentlichten kritische Presseaussendungen und versuchten mehr Informationen durch Anfragen an die Kommission zu erlangen. Erst als auch die Überwachung durch europäische Geheimdienste, etwa durch Tempora und die Datenweitergabe der USA an europäische Dienste thematisiert wurde, wachten auch die EU-Politiker/innen langsam auf.

Immerhin wurde der Überwachungsskandal spontan auf die Tagesordnung der Plenartagung des Europäischen Parlaments Anfang Juni gesetzt. Für die Aufklärung des Skandals setzten sich die Parlamentarier/innen jedoch nur begrenzt ein. Während der 30-minütigen Debatte wurde zwar deutlich, dass einige Fraktionen und Parlamentarier/innen ein ernsthaftes Problem mit der Überwachung hatten, jedoch dauerte es einen weiteren Monat, bis zum 4. Juli, bis sich die Abgeordneten endlich auf eine Resolution einigen konnten. Diese entstand vor allem unter dem Eindruck der kurz zuvor geleakten Information, dass auch EU-Einrichtungen von den USA überwacht wurden. Die Resolution war daher recht ambitioniert und klar in ihren Forderungen: So sollten etwa auch die beiden Datenübermittlungsabkommen für Bank- und Fluggastdaten ausgesetzt werden. Im Parlament sollte sich zudem fortan der Innenausschuss intensiv mit der Aufklärung des Skandals befassen[85]. Dann verschwanden die Parlamentarier/innen in die Sommerpause und weitere Monate mit weiteren Leaks ohne eine ernsthafte Reaktion der EU vergingen. Erst am 5. September traf man sich im Ausschuss, um den Skandal aufzuklären. Zu den geladenen Gästen gehörten etwa Jacob Appelbaum und Duncan Campell[86]. Letzterer veröffentlichte während

seiner Präsentation seine Recherchen über die europäischen Geheimdienste. Campells Informationen zufolge ist Schweden eines der Five Eyes, also eines der Länder, die intensiv an der Überwachung aller Bürger/innen beteiligt sind und als treibende Kraft fungieren. Es schien, als sei es tatsächlich möglich durch den Ausschuss mehr Licht ins Dunkel bringen zu können.

Doch als Bremsklotz erwies sich umgehend die EU-Kommission. Erst am 14. Juni äußerten sich die beiden Kommissarinnen Viviane Reding, zuständig für Justiz, und Cecilia Malmström, zuständig für Inneres, zu dem Überwachungsskandal. Während Reding stolz von ihrem Brief mit allerlei Fragen an den Generalbundesanwalt der Vereinigten Staaten Eric Holder berichtete[87], kündigte Malmström eine transatlantische Expertengruppe an, die von nun an den Skandal aufklären sollte[88]. Noch bevor die Expertengruppe das erste Mal in die USA reisen sollte, wurde offensichtlich, wie sehr die Amerikaner an einer gemeinsamen Arbeit interessiert waren. Denn die von der EU ausgewählten hochrangigen Vertreter mussten sich zunächst einer persönlichen Sicherheitsüberprüfung unterziehen. Man stelle sich vor: Die USA überwacht massenhaft europäische Bürger/innen sowie die Institutionen der EU und statt sich zu entschuldigen, wird die Delegation, die den Skandal aufklären soll, gegängelt. Entsprechend inhaltslos war dann auch das erste Treffen der Gruppe. Die Art. 29 Gruppe etwa äußerte sich in einem Brief an die Kommissarin Reding am 13. August 2013 entsprechend kritisch und verwies auf eine Unzahl bisher nicht beantworteter Fragen, beispielsweise was den Rechtsschutz europäischer Bürger betrifft[89].

Kaum nachvollziehbar ist zudem, dass die Mitglieder der Expertengruppe nicht offiziell bekannt sind. Klar ist nur, dass die Gruppe zweigeteilt wurde. In einem Teil treffen sich die Ermittlungsbehörden und im anderen die Datenschützer. Eine gemeinsame, ernsthafte Aufklärung des Skandals dürfte so kaum möglich sein.

Ein weiteres, zunächst weniger offensichtliches Problem dieser Expertengruppe besteht darin, dass sie den vergleichsweise transparenten Aufklärungsprozess im EU-Parlament verhindert. Denn auf die Einladungen des Ausschusses reagierten die Amerikaner abweisend. Statt sich dem Parlament zu stellen, will man lieber auf die Aufklärung der im Geheimen tagenden Expertengruppe der Kommission zurückgreifen. Doch nicht nur die Amerikaner, auch die EU-Kommission selbst sabotiert die Aufklärungsarbeit des parlamentarischen Ausschusses. Bereits die zweite Sitzung musste teilweise unter Ausschluss der Öffentlichkeit stattfinden, da sich die Kommission nicht öffentlich zu den Leaks äußern wollte[90]. In der dritten Sitzung des Ausschusses waren erneut Vertreter der Kommission vorgeladen. Diese weigerten sich jedoch etwa die Frage zu beantworten, ob durch das Abgreifen von Bankdaten durch die USA – außerhalb des bereits sehr weitreichenden Abkommens zur Übermittlung jener Daten zwischen der EU und den USA – ein Rechtsbruch vorläge. Dieser hätte wohl die Beendigung des Abkommen zur Folge. Und auch die einst ambitionierte Forderung des Parlaments, das Abkommen solange auszusetzen bis man endlich Klarheit über das Ausmaß der Überwachung hat, beantwortete die Kommission verneinend, da man noch nicht ausreichend Informationen vorliegen hätte. Dass der Zweck einer Aussetzung des Bankdatenabkommens genau jener ist, die Fakten zusammenzutragen und dann zu entscheiden, ob man das Abkommen fortführen oder kündigen muss, wurde dabei von der Kommission ebenfalls mit Schweigen goutiert.

Und auch bei der Beantwortung der unzähligen parlamentarischen Anfragen zeigt die Kommission keinen besonders großen Willen, den Skandal aufzuklären. Am Ende bleibt ein zahnloser Ausschuss, der sich im besten Falle deutlich gegen die Überwachung positioniert und vielleicht etwas zur Aufklärung beitragen kann. Leider wird nicht mehr als eine unverbindliche Resolution am Ende durch das Parlament verabschiedet werden können. Ob sich die Kommission an die Forderungen der Parlamentarier hält, darf nach dem bisherigen Vorgehen der Kommissare bezweifelt werden. Neue Fakten durch die transatlantische Expertengruppe kann man zudem nicht erwarten.

Dennoch: Das EU-Parlament ist in Europa offensichtlich die einzige Institution, welche ernsthaft an einer Aufklärung des Skandals interessiert zu sein scheint. Um die Parlamentarier/innen bei dieser Aufklärung zu unterstützen braucht es zivilgesellschaftliches Engagement. Nur so kann die Kommission endlich zur Einsicht bewegt werden. Von allein wird sie kein anderes Gesicht im Skandal zeigen wollen. Nur durch den Druck der Zivilgesellschaft, so haben wir durch ACTA gelernt, kann das Parlament bei seiner Arbeit unterstützt werden und die Kommission zum aktiven Handeln, in dem Fall gegen die Überwachung aller Bürger/innen und sogar internationaler Institutionen zu jeder Zeit, gezwungen werden. Ohne dieses Engagement ist zu befürchten, dass sich die Kommission weiter von den Amerikanern die Bedingungen der Aufklärung diktieren lässt und am Ende keine ausreichend verwertbaren Informationen vorlegen kann, um gegen die gigantische Überwachung aktiv werden zu können.

Wer überwacht die Überwacher?
Geheimdienste außer Kontrolle

Geheimdienste außer Kontrolle: Wer überwacht eigentlich die Überwacher?

Daniel Leisegang

Die Aufgabe von Geheimdiensten besteht in der Ausspähung, Auswertung und Weitergabe von Informationen. Dafür operieren sie in der Regel im Verborgenen. Gerade in einer Demokratie sollten die Dienste daher strenger rechtsstaatlicher Kontrollen unterliegen, sagt Daniel Leisegang. Wer aber prüft, ob sich die Geheimdienste an die geltenden Gesetze halten?

Zahnloser Tiger? Das Parlamentarische Kontrollgremium

Die Nachrichtendienste des Bundes – das Bundesamt für Verfassungsschutz (BfV), der Bundesnachrichtendienst (BND) sowie der Militärische Abschirmdienst (MAD) – werden hierzulande vom Parlamentarischen Kontrollgremium (PKGr) des Deutschen Bundestages kontrolliert. Seine Mitglieder wählt das Parlament zu Beginn der Wahlperiode aus seinen eigenen Reihen. Derzeit gehören dem PKGr elf Bundestagsabgeordnete an[91].

Verfassungsrechtlich ist das Gremium in Artikel 45d des Grundgesetzes verankert, seine konkreten Befugnisse finden sich im »Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes« (Kontrollgremiumgesetz, PKGrG)[92]. Demnach ist die Bundesregierung verpflichtet, das Gremium über die Tätigkeiten der Geheimdienste zu unterrichten[93]. Das PKGr darf zudem Einsicht in einschlägige Regierungsberichte und Geheimdienstakten verlangen, Angehörige der Nachrichtendienste vorladen und Dienststellen besuchen.

Seine weitgehenden Kontrollbefugnisse kann das PKGr zum einen jedoch nur dann wahrnehmen, wenn die Mehrheit seiner Mitglieder dem zuvor auch zustimmt. Da aber die Regierungsvertreter in der Regel die Mehrheit in der PKGr stellen, können sie unangenehme Nachfragen

der Opposition jederzeit unterbinden. Zum anderen erfolgt all dies unter Ausschluss der Öffentlichkeit. Denn die PKGr-Mitglieder sind zu strikter Verschwiegenheit verpflichtet, auch gegenüber anderen Abgeordneten. Nur in Ausnahmefällen können sie mit Zweidrittelmehrheit Sachverständige mit Untersuchungen beauftragen oder kurzzeitig die Schweigepflicht aufheben, beispielsweise um gezielt Informationen zu veröffentlichen.

Neben dem PKGr gibt es noch die sogenannte G10-Kommission. Sie besteht aus vier vom Bundestag ernannten Mitgliedern, von denen derzeit nur eines dem Parlament angehört[94]. Die Kommission entscheidet über die Zulässigkeit von Abhörmaßnahmen. Allerdings tagt auch sie hinter fest verschlossenen Türen.

Damit erfolgt die legislative Kontrolle der bundesdeutschen Geheimdienste weitgehend im Verborgenen. Gerade einmal 12 der insgesamt 620 Bundestagsabgeordneten erhalten detailliertere Informationen über die Tätigkeiten der Dienste – über die sie dann Stillschweigen bewahren müssen.

Das PKGr scheint ein zahnloser Tiger zu sein, denn am Ende müssen sich die Kontrolleure vor allem auf die Angaben der Regierungsvertreter und der Dienste verlassen, deren Wahrheitsgehalt sie nur eingeschränkt überprüfen können. Aus diesem Grund erfuhren sie in der Vergangenheit regelmäßig erst aus den Medien über Rechtsbrüche oder Versäumnisse der Geheimdienste[95].

Großbritannien: Überwachung per Blankoscheck

Aber wie sieht es in anderen Ländern aus – insbesondere in jenen, die in den jüngsten Geheimdienstskandal verwickelt sind?

Einer der mächtigsten Nachrichtendienste in Großbritannien ist das Government Communications Headquarters (GCHQ). Er soll die britische Kommunikations- und Computerinfrastruktur schützen. Seine Aufgabenfelder liegen im Abhören und der Entschlüsselung von Kommunikationsdaten.

Kontrolliert wird der Dienst vom Intelligence and Security Comittee (ISC). Seine neun Mitglieder werden vom britischen Premierminister nominiert und vom Parlament für die Dauer einer Wahlperiode gewählt; sie entstammen beiden Parlamentskammern, dem House of Commons wie auch dem House of Lords[96].

Die Befugnisse des ISC gleichen denen des PKGr: Ihm obliegt die Prüfung des Haushalts, der Verwaltung sowie der Überwachungsmaßnahmen des GCHQ. Dabei kann das ISC Zugang zu geheimen Informationen verlangen und Mitglieder des britischen Kabinetts sowie leitende Angehörige der Geheimdienste befragen. Einmal im Jahr veröffentlicht das Komitee zudem einen Bericht über seine Tätigkeiten, ansonsten tagt es ebenfalls geheim.

Ob diese Kontrollrechte ausreichen, um das mächtige GCHQ im Bann zu halten, darf allerdings bezweifelt werden. Dessen Befugnisse legen vor allem der Intelligence Services Act aus dem Jahr 1994 sowie der Regulation of Investigatory Powers Act (RIPA) aus dem Jahr 2000 fest. Beide Gesetze stammen aus einer Zeit, in der noch nicht abzusehen war, welch große Rolle die digitale Kommunikation über das Internet einmal spielen wird. Sie erteilen dem Dienst weitreichende Rechte, um massenhaft Kommunikationsdaten zu erfassen und auszuwerten.

So wurde erst vor wenigen Wochen bekannt, dass das GCHQ im Rahmen seines Spionageprogramms Tempora mehr als 200 internationale und interkontinentale Glasfaserkabel anzapft, darunter auch das TAT-14 im Atlantik, das einen großen Teil der deutschen Überseekommunikation weiterleitet[97].

Für seine Spähaktionen benötigt das GCHQ nicht einmal eine richterliche Genehmigung. Stattdessen genügt die Generalvollmacht des britischen Außenministers, um umfangreiche Abhörmaßnahmen für die Dauer von sechs Monaten zu autorisieren[98]. Anders wäre die schiere Masse an Überwachungsanträgen vermutlich auch kaum zu bewältigen. Der amtierende britische Außenminister, William Hague, gab erst im Juni zu Protokoll, er prüfe jährlich Hunderte entsprechender Anfragen

des MI6 und des GCHQ. Eine gewissenhafte Einzelprüfung ist da kaum möglich. Die Fülle an Überwachungen sowie die Genehmigungen per Blankoscheck erschweren aber auch die Arbeit des ISC. Denn das Komitee ist somit auf die bereitwillige Unterstützung der Geheimdienste angewiesen – deren Tätigkeit sie eigentlich unabhängig überprüfen soll.

USA: Kontrolle durch ein Schattengericht

Damit entscheiden auch in Großbritannien in erster Linie die Überwacher selbst, wie weit die Kontrolle reicht. Noch düsterer sieht es indes in den USA aus. Denn eine rechtsstaatliche Prüfung der Dienste findet hier nur zum Schein statt.

In enger Kooperation mit dem GCHQ hört der amerikanische Militärgeheimdienst National Security Agency (NSA) ebenfalls den Datenverkehr im Internet ab. Die NSA späht dabei insbesondere Kommunikationsdienste, Soziale Netzwerke sowie Cloud-Speicher aus. Mit einem Jahresbudget von zehn Mrd. US-Dollar und über 30.000 Mitarbeitern ist die NSA der mächtigste der insgesamt zehn US-Geheimdienste.

Die NSA wird vor allem durch zwei Einrichtungen kontrolliert. Zum einen sind die Intelligence Committees des House of Representatives und des US-Senats für die Kontrolle der Finanzen sowie für die Nominierungen der Geheimdienstführung zuständig. Beide Komitees tagen geheim.

Zum anderen muss ein spezieller Gerichtshof sämtliche Überwachungsmaßnahmen gemäß des Foreign Intelligence Surveillance Act (FISA) genehmigen. Innerhalb des amerikanischen Rechtssystems nimmt der Fisa-Gerichtshof (FISC) jedoch eine Sonderstellung ein. Seine Sitzungen wie auch seine Beschlüsse unterliegen grundsätzlich strikter Geheimhaltung. Zudem verhandelt das Gericht ausschließlich Anträge der amerikanischen Regierung. In den Verfahren hört das Gericht dann ausschließlich Mitglieder der US-Administration sowie Angehörige der Nachrichtendienste an[99]. Die Geheimhaltung verhindert jedoch eine

Bewertung der Urteile durch die Presse, den Kongress und die Öffentlichkeit[100].

In seiner 35-jährigen Geschichte hat der FISC rund 99 Prozent der insgesamt rund 34.000 Überwachungsanträge abgenickt. Faktisch ist er kaum mehr als ein Schattengericht, das nur den Anschein von rechtsstaatlicher Kontrolle erwecken soll.

Die Überwachung der Überwacher

Die Parlamente hierzulande, in Großbritannien sowie in den Vereinigten Staaten stehen den jeweiligen Geheimdiensten weitgehend machtlos gegenüber – nicht zuletzt auch deshalb, weil die Regierungen effektive Prüfungen verhindern.

Die deutsche Politik könnte indes mit gutem Beispiel vorangehen und die hiesigen Dienste einer wirkungsvolleren demokratischen Kontrolle unterwerfen. Die Stärkung des Rechtsstaats könnte zum Exportschlager werden, wenn andere Länder es der Bundesrepublik gleichtun, und dem »Wirtschaftsstandort« Deutschland zugute kommen: Denn nicht nur die IT-Branche, sondern nahezu alle Unternehmen sind auf eine Infrastruktur angewiesen, die ihre Daten vor dem unbefugtem Zugriff und damit auch vor Wirtschaftsspionage schützt.

Als erstes müsste das Parlamentarische Kontrollgremium reformiert werden. Deren Mitglieder sollten fortan auch eigenständig die Arbeit der Geheimdienste unter die Lupe nehmen dürfen – ohne dass es dazu einer Mehrheitsentscheidung des Gremiums bedarf. Die Bundesregierung könnte zudem umgehend einen unabhängigen Sachverständigen bestimmen. Seine Hauptaufgabe würde darin bestehen, endlich Licht ins Dunkel des Geheimdienstskandals zu bringen. Dabei sollte er eng mit dem EU-Parlament zusammenarbeiten: Dieses hat bereits Anfang Juli den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres damit beauftragt, die Ausspähung von EU-Bürgern durch den NSA und das GCHQ sowie anderer Dienste zu untersuchen.

Langfristig ist entscheidend, dass an die Stelle des unkontrollierten digitalen Abhörkomplexes völkerrechtlich abgesicherte Strukturen für

eine freie, ungehinderte Kommunikation treten. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, hat dahingehend bereits einen ersten Vorschlag gemacht: die Einführung eines Zusatzprotokolls zu Artikel 17 des UN-Paktes für bürgerliche und politische Rechte, der den Einzelnen vor willkürlichen oder rechtswidrigen Eingriffe in sein Privatleben schützt. Staaten, die sich nicht zu diesem bekennen, müssten dann nachweisen wie sie trotzdem Datenschutz, Privatsphäre und Fernmeldegeheimnis garantieren.

Den Regierungen sollte klar sein, dass ein Staat, der seine eigenen Bürger (und die Bürger anderer Staaten) systematisch ausspioniert, nicht nur das Vertrauen in seine Nachrichtendienste, sondern am Ende auch in die Demokratie selbst untergräbt. Um eine solche Entwicklung zu verhindern hilft nur eines: die transparente, rechtsstaatliche Überwachung der Überwacher.

Dieser Artikel erschien zuerst am 13. September 2013 in der Netzdebatte* der bpb[101].*

Die notwendige Kontrolle des Sicherheitsstaates

Prof.Dr.Andreas Busch

Seitdem die britische Tageszeitung *The Guardian* am 9. Juni 2013 die ersten Enthüllungen des ehemaligen NSA-Angestellten Edward Snowden über die Spionageaktivitäten verschiedener Geheimdienste veröffentlicht hat, hat sich vieles verändert. Man ist seitdem nicht mehr der Paranoia verdächtigt, wenn man die enorm angestiegenen Aktivitäten von Geheimdiensten und Sicherheitsapparat in liberalen Demokratien problematisiert und auf die Notwendigkeit einer genaueren Kontrolle hinweist. Seit die amerikanische, britische und auch die deutsche Regierung durch Nicht-Dementis viele der von Snowden mithilfe elektronischer Dateien aufgestellten Behauptungen mehr oder weniger bestätigt haben, ist bei vielen Menschen das Bewusstsein gewachsen, dass eine Reihe von Dingen nicht so gelaufen sind wie sie sollten und unsere Demokratien ein ernstes Problem haben.

Muss man deshalb denjenigen glauben, die unsere Demokratie bereits zentral gefährdet sehen, ja von einem »historischen Angriff auf unseren demokratischen Rechtsstaat« sprechen, wie das eine Reihe von Autoren in einem Offenen Brief an die Bundeskanzlerin getan haben? Die Antwort darauf ist ein klares Nein. Die etablierten liberalen Demokratien, wie die Bundesrepublik eine ist, sind stabil und sind verteidigungsfähig – und sie sind das auch, wenn die Affären um die verschiedenen Abhör- und Überwachungsskandale nicht die elektorale Aufmerksamkeit erlangt haben – etwa im bundesdeutschen Wahlkampf im Sommer und Herbst 2013 –, die sich die Aktivisten der »Netzgemeinde« erhofft haben. Deren Enttäuschung ist zwar verständlich, aber sie ist nicht überraschend; und sie ist auch kein Grund zur Sorge. Denn die »Netzgemeinde« neigt seit jeher zur Nabelschau und überschätzt ihre eigene Wichtigkeit. Wenn der Rest der Bevölkerung in seiner Mehrheit diese Sorgen nicht mit derselben Emphase teilt, dann ist das wenig verwunderlich.

Können und sollten wir also zur Tagesordnung übergehen, müssen wir uns keine Sorgen machen? Darauf allerdings gibt es ein ebenso emphatisches Nein. Die im Gefolge der Enthüllungen von Edward Snowden bekannt gewordenen Überwachungs- und Ausforschungsprogramme sind von einem Ausmaß und einer so umfassenden Natur wie dies sich auch viele kritische Beobachter dieses Bereichs nicht haben vorstellen können. Es ist offenkundig: Teile des Sicherheitsstaates sind außer Kontrolle geraten und haben ein Eigenleben entfaltet. Es zeigt sich, dass Mechanismen der exekutiven und parlamentarischen Kontrolle eindeutig nicht so funktionieren wie das intendiert ist. Dass dieses in seinem Ausmaß über den verschiedenen betroffenen Länder variiert und dass nur in einigen Ländern das Geschehen mit stillschweigendem Einverständnis von Teilen der Exekutive stattgefunden zu haben scheint, macht die Sache nicht besser.

Apodiktische Urteile über die Verwerflichkeit des Geschehenen sind jedoch ebenso wenig hilfreich wie Verschwörungstheorien. Stattdessen ist kühle Analyse des Geschehenen gefragt – und sie ist sowohl möglich wie auch nötig. Dieser Aufsatz soll ein Beitrag zu einer solchen Analyse sein. Vielleicht kann er zu der notwendigen Debatte ein paar Gedanken beitragen.

Die Entwicklung des Präventivstaates

Um staatliches Handeln zu verstehen, ist ein Blick auf die ideellen Grundlagen und das Selbstverständnis des Staates instruktiv. Im Bereich Sicherheit/innere Sicherheit lässt sich hier eine paradoxe Überentwicklung des Präventivstaats konstatieren, die Gefahr läuft, die Grundlagen liberaler Demokratie zu beschädigen. Die Idee des »Vorsorgeprinzips« sowie des präventiven Handelns als Leitidee kommt ursprünglich aus dem Bereich der rechtlichen Regulierung technischer Sicherheit und des Umweltschutzes. Von dort hat sie sich in viele andere Rechtsbereiche ausgebreitet; ein besonderes Gefährdungspotenzial entwickelt dieser Ansatz allerdings im Bereich der inneren Sicherheit, wo er Gefahr läuft, die für die liberale

Demokratie essentiellen Einschränkungen exekutiver Staatsmacht zu untergraben.

Natürlich hat es auch in der Vergangenheit für die staatliche Polizeigewalt die Möglichkeit gegeben, präventiv zu handeln. Doch war dieses jeweils immer auf »konkrete Gefährdung« der öffentlichen Sicherheit beschränkt, die auf einem individuellen Verdacht zu beruhen hatte. Mit der Verschiebung in Richtung Prävention gewann in der Gesetzgebung jedoch die Beschreibung von Zielen Oberhand gegenüber der Beschreibung konkret zu unternehmender Maßnahmen. Als Folge, so haben das Staatsrechtler wie Erhard Denninger oder Dieter Grimm bereits in den 1990er Jahren kritisch beschrieben, kommt es zu einem Ansteigen staatlicher Macht und einer Verringerung des Schutzniveaus für den einzelnen Bürger gegen staatliches Handeln, da das Schutzgebot des Staates nun von der konkreten auf die potenzielle Gefahr ausgeweitet wird[102][103].

Der klassische Rechtsstaat sanktioniert Verhalten, das gesetzliche Regeln verletzt; der Präventivstaat hingegen versucht, bereits die Normverletzung zu verhindern. Er wird so zum Rechtsgüterschutzstaat. Um dies sein zu können, muss er jedoch umfassende Informationen über seine Bürger sammeln, die damit alle zu potenziellen Normenverletzern werden. Der Bürger mutiert somit vom zu schützenden Subjekt zum potenziell Verdächtigen.

Transformationen des Sicherheitsstaates

Die Terroranschläge vom 11. September 2001 in den Vereinigten Staaten von Amerika waren ein weltweiter Schock, der in fast allen Staaten zu einer massiven Ausweitung der Tätigkeit im Bereich innere Sicherheit geführt hat und viele Schranken, die das Verhältnis zwischen dem einzelnen Bürger und dem Staat reguliert haben, niedergerissen hat. Ein umfassender Trend in Richtung »Securitisierung« führte zu einem Ausbau staatlicher Tätigkeit, der sich in drei großen Veränderungen zusammenfassen lässt: dem Verschwimmen der Trennung zwischen innerer und äußerer Sicherheit; dem Verschwinden der Trennung zwischen Polizei-, Geheimdienst- und Militärarbeit; sowie der massiven

Zunahme der Rolle von Informations- und Kommunikationstechnologien.

Die Verwischung der Trennung zwischen dem Innen und dem Außen

Obwohl die am 11. September 2001 als Waffen gebrauchten Verkehrsflugzeuge auf dem Territorium der Vereinigten Staaten gestartet waren, wurden die Anschläge als Angriff von außen wahrgenommen – sowohl in den Vereinigten Staaten wie auch von der internationalen Gemeinschaft. Da es sich bei den Terroristen um ausländische Staatsangehörige handelte, hatte diese Interpretation eine gewisse Plausibilität. Es war jedoch auch klar, das gegen eine solche Bedrohung klassische Abwehrmechanismen gegen auswärtige Bedrohungen (wie Armeen, Flugzeuge oder Schlachtschiffe) wenig würden ausrichten können; die Verteidigung hatte vielmehr an der Landesgrenze zu erfolgen, an Grenzübergängen, in Häfen und auf Flughäfen.

Eine Fortifizierung der Landesgrenzen war die Folge und damit wurde ein Trend umgekehrt, der über viele Jahrzehnte Bestand gehabt hatte: denn im Zuge der wachsenden internationalen wirtschaftlichen Verflechtung waren Grenzen durchlässiger geworden und Grenzkontrollen hatten abgenommen[104]. Nun wurden die Grenzen mit großem Aufwand an Personal und Material zu Sicherheitszonen gemacht, mit einem erheblichen Anwachsen von vorherigen Überprüfungen sowie dem Einsatz massiver Computer- und Datenbanksysteme.

Die Zusammenführung von Polizei-, Geheimdienst- und Militäraufgaben

Die Verwischung zwischen innerer und äußerer Sicherheit hatte auch Folgen für die Instrumente, mit denen der Staat Sicherheit zu produzieren sucht. Die klassische Aufgabenteilung zwischen Polizeiarbeit (Durchsetzung der Gesetze), inländischer Geheimdienstarbeit (Schutz der verfassungsmäßigen Ordnung) und

militärischen Aufgaben (Schutz vor auswärtiger Bedrohung) begann sich aufzulösen. In den USA wurde das unter dem Stichwort »Homeland Security« diskutiert, in der Bundesrepublik als »Neue Sicherheitsarchitektur«. Zur Rechtfertigung wurde die Größe der Aufgabe und die daraus folgende Notwendigkeit einer Zentralisierung von Kompetenzen angeführt. Da Informationen eine zentrale Rolle spielten, musste eine einheitliche Organisationsstruktur für umfassenden und konsistenten Zugang zu Daten sorgen – nur so konnte der Staat effektiven Schutz organisieren. Nicht überall hat das zu so drastischen organisatorischen Konsequenzen geführt wie in den Vereinigten Staaten: dort wurden 22 Behörden mit 180.000 Beschäftigten (vom Zoll über die Grenzsicherung bis zur Küstenwache und dem Geheimdienst) unter einem neuen Ministerium für »Homeland Security« zusammengefasst[105]. Auch in Deutschland bekam das Bundeskriminalamt zahlreiche neue Kompetenzen und in Großbritannien wurde ein gemeinsames Terrorismusanalysezentrum gegründet; ähnliche Entwicklungen gibt es in den meisten anderen OECD-Ländern. Aber nicht nur im staatlichen Sektor entstehen so große Akteure, die ein erhebliches Eigeninteresse an der Ausweitung staatlicher Sicherheitsproduktion haben: auch im privaten Bereich ist eine »Sicherheitswirtschaft« (so die Bezeichnung in einem Bericht der OECD aus dem Jahr 2004) entstanden, die auch schon als »Überwachungs-industrieller Komplex« gekennzeichnet worden ist[106]. Die Größe dieses Wirtschaftssektors wurde bereits vor zehn Jahren auf jährlich zwischen 100 und 120 Milliarden US-Dollar geschätzt[107].

Zunehmende Wichtigkeit von Informations- und Kommunikationstechnologie

Parallel zur Zunahme der Verwendung von Informations- und Kommunikationstechnologien (ICT) in der gesamten Gesellschaft hat sich über die letzten zwei Jahrzehnte auch deren Benutzung durch die Sicherheitsbehörden ausgeweitet. Gigantische Kapazitäten zur Datenspeicherung und zur Verknüpfung dieser Daten sind entstanden und das Vertrauen auf solche Daten als primäre Informationsquelle ist

dominant geworden. Staaten haben bereits existierende Datenquellen zusammengeführt, um ihre Grenzen besser bewachen zu können: Visa-Systeme, Überwachungslisten für Kriminelle, Passagierdaten von Fluglinien und mit RFID-Chips ausgerüstete Pässe spielen dabei neben anderen eine Rolle[108]. Viele Staaten erfassen ihre Bürger auch über Proben des Erbguts und genetische Profile, die sie von Kriminellen oder der Kriminalität Verdächtigen entnehmen. Großbritannien beispielsweise führt mit 7 Millionen DNA-Profilen (das ist jeder neunte Einwohner!) gegenwärtig mit einigem Abstand die entsprechende Liga an[109]. Und existierende Datenbanken werden miteinander verbunden, wie beispielsweise in Deutschland, wo eine neue Anti-Terrordatei 334 vormals separate Datenbanken zusammengeschaltet hat und zudem 511 Protokolldateien allen Mitarbeitern von 38 unterschiedlichen staatlichen Agenturen zugänglich gemacht hat[110]. Ob dieses enorme Anwachsen von zugänglicher Information tatsächlich funktional ist für die Lösung des Sicherheitsproblems, kann man jedoch bezweifeln: Informationsüberflutung gilt als ein zentrales Problem im Kampf gegen Terrorismus[111]; und schon nach dem 11. September 2001 wurde betont, dass es nicht der Mangel an Information, sondern vielmehr der Mangel an Analyse der Information gewesen sei, der diese Angriffe möglich gemacht habe[112].

Terrorismus als Problem

Der Kampf gegen Terrorismus ist vor allem ein Kampf gegen die Angst. Schon 2003 hat der amerikanische Politikwissenschaftler Peter Katzenstein das politische Problem des Terrorismus als eines der »Bedrohungsvergrößerung« (*threat magnification*) beschrieben[113]. Nach dem 11. September 2001 haben sich die meisten liberalen Demokratien diesem Problem der »Bedrohungsvergrößerung« ergeben und praktisch in einem permanenten Zustand der Terrorismusbedrohung existiert.

Als objektive Gefahr ist der Terrorismus (als Todesursache) schon immer statistisch unbedeutend gewesen, darüber herrscht in der

Literatur Einigkeit[114] [115]. Die Zahl der Todesfälle etwa durch Hirnhautentzündung, Mord oder gar Autounfälle übersteigt diejenigen durch Terrorismus um ein Vielfaches. In Großbritannien ist sogar von offizieller Stelle ausgerechnet worden, dass dort seit dem Jahr 2000 jährlich im Durchschnitt fünf Tote durch internationalen Terrorismus zu beklagen sind, was exakt der jährlichen Todesrate durch Hornissen-, Bienen- und Wespenstiche und lediglich einem Sechstel der Zahl derer entspricht, die den Tod durch Ertrinken in der eigenen Badewanne gefunden haben[116].

Die enorme Ausweitung, die sich (insbesondere seit »9/11«) in Bezug auf das Personal, die Gesetzgebung und die Ausgaben für den Kampf gegen den Terrorismus und die innere Sicherheit ergeben haben, stehen also in einem markanten Kontrast zur objektiven Gefährdung. Wir sind mit dem Paradoxon konfrontiert, dass der Staat sich in vielen Bereichen schon seit längerem aus Tätigkeiten zurückzieht, diese delegiert oder privatisiert. Politikwissenschaftler, die sich mit dem Wandel von Staatlichkeit beschäftigen, sehen den Staat auf dem Weg vom »Herrschaftsmonopolisten« zum »Herrschaftsmanager«[117]. Diese Entwicklung trifft jedoch offenkundig nicht auf den Bereich des Sicherheitsstaates zu. Hier weist der staatliche Aufwand nicht nach unten, sondern eindeutig nach oben – und es ist auffällig, in welchem Maße es den Handelnden im Bereich des Sicherheitsstaates gelungen ist, ihre Prioritäten der Gesellschaft aufzudrücken. Dies ist insbesondere bemerkenswert im Angesicht von wirtschaftlichen Krisen, Austerität und genereller Sparsamkeit.

Eine kühle Analyse dieser Entwicklungen ist ebenso möglich wie eine Kontrolle in diesem Bereich notwendig ist. Die Aufdeckungen der letzten Monate haben gezeigt, dass im Bereich der inneren Sicherheit, der Geheimdienste und der Polizeibehörden vieles im Argen liegt und bessere Kontrolle notwendig ist. Je unaufgeregter Analyse und Kritik vorgehen, je klarer sie sich orientieren an den Grundlagen der liberalen Demokratie und deren Einhaltung einfordern, desto eher – das ist zu

hoffen und zu erwarten – besteht eine Chance, dass damit auch politisch Gehör gefunden wird.

Dieser Aufsatz, geschrieben im Oktober 2013, nimmt einige Überlegungen auf, die der Autor in einem Beitrag für das Oxford Handbook of Transformations of the State,[118] *ausführlicher entwickelt hat.*

Geheimdienste und Bürgerrechte

Thomas Stadler

Die Enthüllungen Edward Snowdens werfen unzählige Fragen auf. Eine davon lautet: Wie verträgt sich die Tätigkeit von Geheimdiensten mit der Vorstellung von global geltenden Bürger- und Menschenrechten? (Auslands-)Geheimdienste sind ein Relikt aus dem 20. Jahrhundert. In der Zeit des Kalten Krieges wurde es als politische Notwendigkeit angesehen, dass sich Staaten, nicht nur wenn sie verfeindet waren, gegenseitig bespitzeln. Dieser Legitimationsansatz ist längst weggefallen. Nach den Anschlägen des 11. Septembers 2001 wurde er durch einen anderen ersetzt, nämlich den der Terrorbekämpfung. Dass Geheimdienste daneben aber auch Wirtschaftsspionage betreiben, ist mittlerweile mehr als ein offenes Geheimnis. James R. Clapper, Director of National Intelligence, hat dies in einem offiziellen Statement eingeräumt, indem er darauf hinwies, dass Geheimdienste Informationen über ökonomische und finanzwirtschaftliche Angelegenheiten sammeln, u.a. auch um Einsichten in die Wirtschaftspolitik und das wirtschaftliche Verhalten anderer Staaten zu erlangen.

Der Tätigkeit von Geheimdiensten, egal welches Ziel sie verfolgen, liegt eine letztlich widersprüchliche Logik zu Grunde. Geheimdienste werden weltweit – immer von einer national geprägten Sichtweise aus – als legitim betrachtet, obwohl ihr Auftrag am Ende darin besteht, Politiker, Unternehmen und mittlerweile auch Bürger fremder Staaten zu überwachen und damit auch das Recht dieser Staaten zu brechen.

Dieses an sich bereits merkwürdige Konstrukt erweist sich im Zeitalter eines weltumspannenden Datennetzes endgültig als Anachronismus. Mit der Vorstellung von global geltenden Bürger- und Menschenrechten war es ohnehin nie wirklich vereinbar. Denn die Verletzung des Rechts fremder Staaten durch Geheimdienste beinhaltet immer auch die Verletzung der Grundrechte der Bürger dieses Staates. Der amerikanische Politberater Andrew B. Denison hat dies in der Talkshow

von Anne Will auf den Punkt gebracht, indem er sagte, es sei die Aufgabe der NSA, das Recht fremder Staaten zu brechen, allerdings nicht, ohne dies praktisch im selben Atemzug als legitim zu bezeichnen. Wenn wir ein weltweites System von Geheimdiensten akzeptieren, dann akzeptieren wir auch immer auch die weltweite Verletzung von Grund- und Bürgerrechten.

Die aktuelle öffentliche Diskussion erfasst die Tragweite und Bedeutung dieses Aspekts noch nicht ansatzweise. Wir müssen die Rolle der Geheimdienste vor dem Hintergrund der Funktionsfähigkeit desjenigen Staatswesens diskutieren, zu dem sich alle westlichen Staaten formal bekennen. Verträgt sich das Grundkonzept von Geheimdiensten mit der Vorstellung von einer freiheitlich-demokratischen Grundordnung? Die nationalstaatliche Betrachtungsweise ist dafür zu eng. Andernfalls würden wir akzeptieren, dass das Recht eines beliebigen Nationalstaats im Ergebnis immer Vorrang vor global geltenden und wirkenden Menschen- und Bürgerrechten hätte.

Wir müssen letztlich erkennen, dass unser Demokratisierungsprozess noch nicht abgeschlossen war, sondern vielmehr gerade ins Stocken geraten ist. Auf dem Weg zu einer vollständigen freiheitlich-demokratischen Grundordnung müssen Fremdkörper wie Geheimdienste beseitigt werden. Sie sind Ausdruck eines archaisch-kriegerisch geprägten Denkens, das es zu überwinden gilt. Man kann durch nationales Recht den Bruch des Rechts eines anderen Staates nicht legitimieren. Es handelt sich dabei vielmehr um die Fortsetzung des Kriegs mit anderen Mitteln.

Geheimdienste bewirken die Entstehung rechtsfreier Räume, die weltweit niemand mehr kontrollieren kann. Denn die Geheimdienste, zumindest die formal befreundeter Staaten, tauschen ihre Erkenntnisse wiederum wechselseitig aus, und umgehen damit aktiv die Bindungen ihres nationalen Rechts. Was sie selbst nicht ermitteln dürfen, erledigt ein ausländischer Geheimdienst, der die Daten und Informationen liefert, die für den jeweils nationalen Dienst tabu sind. Geheimdienste schaffen dadurch ein weltweit vernetztes und unkontrolliert agierendes System, das der zielgerichteten Aushebelung von Bürgerrechten dient.

Es kommt hinzu, dass das Internet die Rahmenbedingungen entscheidend verändert hat. Denn mit der Überwachung durch Geheimdienste ist es so ähnlich wie mit dem Urheberrecht. Was in den 80er Jahren noch auf einen kleineren Personenkreis beschränkt war, betrifft plötzlich (nahezu) alle Menschen.

Viele Bürger haben mit dieser Überwachung offenbar deshalb kein Problem weil sie glauben, das würde sie nicht betreffen, sondern nur Terroristen oder Terrorverdächtige. Warum diese Annahme naiv und falsch ist, lässt sich im Grunde mit einem Wort erklären: Guantanamo. Dort werden seit Jahren Menschen festgehalten, die zu einem erheblichen Teil unschuldig sind und die nie ein ordentliches Gerichtsverfahren bekommen haben und auch nie eines bekommen werden. Es kann also im Grunde jeder in den Fokus von Geheimdiensten und Sicherheitsbehörden geraten, wenn man zur falschen Zeit am falschen Ort ist, oder wenn die digitale Rasterfahndung aus ein paar ungünstigen Einzelindizien einen unberechtigten Tatvorwurf entstehen lässt. Dieses Phänomen kennt man sogar aus Strafverfahren, die vergleichsweise strikten rechtsstaatlichen Vorgaben folgen. Spätestens dann, wenn es keine nachvollziehbaren Regeln mehr gibt und die Betroffenen überhaupt nicht mehr wissen, welche Einzelinformationen gesammelt wurden und wie diese verknüpft worden sind, wird der Einzelne zum Objekt eines undurchsichtigen Machtapparats. Genau vor dieser Entwicklung sollen uns die Grundrechte schützen, aber sie tun es nicht mehr. Es geht längst nicht mehr nur um einzelne Grundrechte, wie die informationelle Selbstbestimmung oder das Fernmeldegeheimnis. Es geht um die Würde des Menschen, um das Recht, selbstbestimmtes Subjekt sein zu dürfen, das sich von nichts und niemand zum bloßen Objekt einer undurchsichtigen Überwachungsmaschinerie machen lassen muss.

Die aktuelle Entwicklung führt zu der Frage, für welches Menschenbild unsere Gesellschaft künftig stehen wird. Für das des Subjekts, das frei und selbstbestimmt handeln kann oder für das des Objekts, das unter dem Vorwand der Sicherheit bloßer Spielball eines Staates bleibt. Derzeit gaukelt man uns weiterhin das Ideal von der freien Entfaltung der Persönlichkeit in einem freiheitlich-demokratischen Staat vor,

während im Hintergrund die Geheimdienste verschiedenster Staaten unsere Kommunikation nahezu lückenlos überwachen bzw. eine solche Überwachung zumindest anstreben. Beide Aspekte sind miteinander unvereinbar.

Gegen diese auf die Förderung und den Ausbau von Geheimdienstaktivitäten gerichtete Politik hilft einzig und allein Öffentlichkeit und Transparenz. Man kann insoweit auf die von Kant formulierte transzendentale Formel des öffentlichen Rechts zurückgreifen, die lautet:

> *»Alle auf das Recht anderer Menschen bezogene Handlungen, deren Maxime sich nicht mit der Publizität verträgt, sind unrecht.«*

Laut Kant wird sich der ewige Frieden zwischen den Völkern nur dann einstellen, wenn im öffentlichen Bereich eine größtmögliche, ja sogar radikale Publizität herrscht.

Edward Snowden und Chelsea Manning stehen in dieser Tradition der Aufklärung, während mächtige Strömungen in der internationalen Politik ihr entgegen arbeiten. Snowden hat den Bruch von Bürger- und Menschenrechten offenkundig gemacht, zu denen sich formal alle Staaten der westlichen Welt bekennen. Aus Sicht des Rechts, zumindest wenn man es global betrachtet und nicht national, ist Snowden deshalb kein Verräter, sondern ein Aufklärer. Der Rechtsbruch, der ihm vorgeworfen wird, besteht darin, auf einen global wirkenden Rechtsbruch hingewiesen zu haben. Weil er sich damit aber die US-Administration zum Feind gemacht hat, wird er gejagt und kein europäischer bzw. westlicher Staat war bereit, ihm Asyl zu gewähren, obwohl seine politische Verfolgung offensichtlich ist.

Die weltweite Geheimdienstaffäre wirft in letzter Konsequenz die Frage nach dem Zustand unserer westlichen Demokratien auf. Nicht mehr und nicht weniger. Die Qualität eines freiheitlich-demokratischen Staates zeigt sich nämlich gerade auch am Umgang mit Aufklärern wie Snowden oder Manning, die zu Unrecht als Verräter denunziert, verfolgt und ihrer Freiheit beraubt werden. Es besteht derzeit wenig Grund zu der Annahme, dass die Politik bereit und in der Lage dazu ist, die

Geheimdienste unter rechtsstaatliches Kuratel zu stellen. Es wird also alles von den Bürgern abhängen, die selbst für ihre Rechte eintreten und kämpfen müssen.

Rechtsrahmen für geheimdienstliche Überwachung im Internet: USA, Großbritannien und Deutschland im Vergleich

Stefan Heumann, Ben Scott

Viele Europäer sind entsetzt über das Ausmaß der staatlichen Überwachungsprogramme der USA, die in den von Edward Snowden enthüllten NSA-Dokumenten dokumentiert sind. Deutsche und europäische Politiker und Regierungsvertreter haben die US-Regierung scharf für die Mißachtung der Privatsphäre europäischer Bürger und die Ausspähung ihrer persönlichen Daten und ihrer Kommunikation kritisiert. Die Sorge über das Ausmaß der Internetüberwachung durch die NSA und andere Geheimdienste ist berechtigt (gestrichen sicherlich). Und Kritik von engen Partnern und Verbündeten ist wichtig, um Druck auf die US-Regierung auszuüben, damit sie die Reichweite dieser Programme neu bewertet und einen Reformprozess beginnt mit dem Ziel, die Aufsicht und Rechenschaftspflicht zu stärken. Um glaubwürdig für Reformen einzutreten, müssen Europäer ihre eigenen Geheimdienste allerdings den gleichen Standards unterwerfen, die sie von anderen Regierungen fordern. Und sie müssen transparent machen, welche Standards das sind und wie sie in der Praxis angewendet werden. Die schärfsten Kritiker der US-Regierung kommen unter anderem aus Deutschland. Diese Kritiker nehmen implizit an, dass Deutschland höhere Standards zur Kontrolle und Begrenzung seiner Geheimdienste habe als die USA. In diesem Beitrag überprüfen wir diese Annahme, indem wir die der geheimdienstlichen Überwachung zu Grunde liegenden Gesetze in den USA, Großbritannien und Deutschland vergleichen, die die auf Nicht-Bürger abzielende elektronische Aufklärung regulieren.

Wir konzentrieren uns hierbei auf drei Analysebereiche:

1. Rechtliche Grundlagen für Überwachungsprogramme;
2. Funktionsumfang und Anwendungsbereich der Datensammlungen; und

3. Maßnahmen zur Aufsicht und Rechenschaftspflicht, um die Programme zu beschränken und zu kontrollieren.

Die hier stattfindende Auseinandersetzung versteht sich nicht als umfassende Prüfung aller relevanten Aspekte, sondern als sorgfältige Skizzierung der rechtlichen Rahmenbedingungen und Maßnahmen, die einen aussagekräftigen Vergleich ermöglichen. Der Vergleich hat das Ziel, eine Analyse nationaler Überwachungsregularien zu bieten und basierend auf der vergleichende Analyse mögliche Reformansätze zu identifizieren, um neue transatlantische Richtlinien abzustimmen, die die Balance zwischen für unsere Sicherheit notwendiger elektronischer Überwachung und dem Recht auf Privatsphäre wieder herstellen.

Unsere Ergebnisse widersprechen der These, dass die auf das Ausland zielenden Programme des amerikanischen Auslandsgeheimdienst NSA auf grundlegend anderen politischen Entscheidungen basieren als die geheimdienstlichen Programme von zwei ihrer größten europäischen Verbündeten. Es ist sicherlich korrekt, dass die NSA-Programme in breiterem Umfang angewendet werden als die anderer Regierungen. Und die US-Geheimdienstbehörden haben zudem den Vorteil, die größten globalen Internet-Dienstleister zur Kooperation zwingen zu können, denn viele von ihnen sind US-Firmen. Dennoch scheint es mehr Ähnlichkeiten als Unterschiede zwischen den drei Ländern zu geben, wenn man die Autorisierung der Programme, ihre Funktionsweise und die bestehenden Aufsichtsmechanismen betrachtet. Die Gesetze, die zur digitalen Überwachung berechtigen, haben eine gemeinsame Struktur, auch wenn die Interpretation, wie sie anzuwenden sind, sich unterscheiden mag.

Die Reichweite der internationalen Kooperationen der NSA und die Ausmaße ihrer Programme machen klar, dass eine Reformdebatte in Washington notwendig und dringend geboten ist. Aber die US-Richtlinien unterscheiden sich nicht in ausreichendem Maße von denen ihrer Verbündeten, um zum Beispiel den rechtlichen Rahmen in Deutschland oder Großbritannien als Grundlage für die Entwicklung internationaler Normen zu nehmen. Unsere vorläufige Analyse legt nahe, dass die derzeitig vorherrschenden Rechtsrahmen sich viel

weniger von US-Richtlinien unterscheiden, als die aktuelle Debatte vermuten lässt. In allen drei Ländern genießen die Geheimdienstbehörden große Diskretion und Unabhängigkeit bei der Sammlung ausländischer Informationen. Legale Beschränkungen und Aufsichtsmechanismen beschäftigen sich hauptsächlich mit dem rechtlichen Schutz der eigenen Bürger. Und oftmals werden diese Einschränkungen erst nach dem Abhören und der Sammlung des Telekommunikationsverkehrs wirksam. Die Unterschiede in den Strukturen der Handlungsrichtlinien lassen die USA nicht alleine in schlechtem Licht dastehen. Zum Beispiel fehlt es allen drei Ländern an verlässlichen Systemen zur rechtlichen Kontrolle der Geheimdienste, um die Bürger vor unzulässiger Überwachung zu schützen. Nur die USA beziehen Gerichte in die Autorisierung mancher Programme mit ein. Die deutsche G10-Kommission, eine Aufsichtsbehörde des Parlaments, nimmt eine ähnliche, wenn auch nicht-richterliche Rolle, ein wie der amerikanische FISA-Gerichtshof. Aber ihr Handlungsrahmen und Auftrag ist umfassender. Großbritannien hat die schwächsten Aufsichtsmechanismen., Es fehlt an institutionalisierter Prüfung von Überwachungsprogrammen, sowohl von Seiten der Legislative als auch der Judikative. Die eigentliche Arbeit der mit der Aufsicht und Genehmigung der Überwachungsprogramme betrauten Einrichtungen liegt in allen drei Ländern unter einem Schleier der Geheimhaltung.

Diese Studie versucht, eine Grundlage für einen internationalen Dialog auf Basis der Fragen nach den rechtlichen Rahmen der Überwachung anzustoßen. Ohne diese Debatte und die daraus zu ziehenden Konsequenzen sehen wir kaum Chancen, wie das Vetrauen der Bürger in digitale Kommunikation wieder hergestellt werden kann. Um den Umfang des Berichts überschaubar zu halten, wird sich die Analyse auf die Überwachungsprogramme von Geheimdiensten konzentrieren, die auf Nicht-Bürger abzielen. Jedoch verschwimmen in allen drei Fallstudien die Regelungen bezüglich der Überwachung im eigenen Land und außerhalb seiner Grenzen bedingt durch das Wesen der Technologie und die Methoden der Datenerhebung und -analyse. Das bedeutet, dass die Unterscheidung zwischen ausländischer und inländischer Internetkommunikation schwer vorzunehmen ist. Selbst

das, was wir als inländische Kommunikation von zwei Bürgern betrachten würden, die innerhalb der geographischen Grenzen ihres Heimatlandes miteinander in Kontakt treten, könnte durch Server in der ganzen Welt geleitet und ihre Kommunikationsdaten könnten im Ausland gespeichert und verarbeitet werden. Daher gewinnen auch Geheimdienstoperationen, die sich auf ausländische Kommunikationsinfrastrukturen fokussieren, gezwungenermaßen Informationen über die eigenen Bürger. Zweitens zeigen die geleakten Dokumente, dass es eine intensive Zusammenarbeit zwischen den Geheimdiensten der USA, Großbritanniens und Deutschlands gibt. Das gibt diesen Geheimdienstbehörden ein breites Spektrum an Möglichkeiten, durch internationale Zusammenarbeit und Datenaustausch Einschränkungen ihrer Heimatländer zu umgehen. Zieht man die internationalen Reichweite dieser Programme in Betracht, ergeben inländische Reformen wenig Sinn, wenn sie nicht an internationale Reformbemühungen geknüpft sind. Die Schlüsselfrage ist, ob der rechtliche Schutz, der Bürgern gewährt wird, auf bestimmte Gruppen von Nicht-Bürgern ausgeweitet werden sollte und wenn ja, ob diese Reformen politisch möglich und technisch durchführbar sind. Der Ausgangspunkt zur Beantwortung dieser Fragen beginnt mit dieser Analyse.

USA

Rechtliche Autorisierung

Mehrere unterschiedliche Statuten dienen als Grundlage für die Autorisierung der geheimdienstlichen Informationssammlung in den USA. Die Komplexität dieser Programmkonstellationen und die einzelnen Berichte über die Snowden-Dokumente verhindern oftmals den Blick auf den größeren Zusammenhang. Das macht es so schwierig, die technische Funktionsweise jedes Programms und die passenden Gesetze, die diese Programme autorisieren und beaufsichtigen, in Einklang zu bringen. Um die Sache zu vereinfachen sollten wir zwischen zwei grundlegende Überwachungsansätzen unterscheiden. Beide Ansätze finden sich in den Programmen der meisten Geheimdienste, die Überwachung im Internet durchführen, wieder.

Der erste Ansatz ist das Abfangen von Echtzeitinformationen direkt an den Kabeln der Telekommunikationsnetzwerke. Das reicht vom Abhören einer einzigen Leitung bis zur Speicherung des gesamten »Upstreams« massiver Mengen von Internet- und Telefonverkehr, die von Computersystemen umgeleitet und gespeichert werden, um sie nachträglich zu analysieren. Der zweite Ansatz ist die Sammlung von Daten, die auf Computern oder Servern von Organisationen oder Unternehmen gespeichert sind. In beiden Fällen erfolgt der Zugriff typischerweise durch das Vorzeigen einer verbindlichen Rechtsanordnung bei einem kommerziellen Anbieter, der Daten überträgt, speichert oder verarbeitet. Der Foreign Intelligence Surveillance Act (FISA) und seine Änderungen sind die zentralen Bestandteile gesetzlicher Berechtigung für die auslandsgeheimdienstliche Ermittlung von Informationen durch elektronische Überwachung. Diese Gesetze berechtigen beide Ansätze der Datensammlung. Abschnitt 215 des US PATRIOT Act betrifft auch die Ermittlungen von Auslandsgeheimdiensten. Er berechtigt dazu, eine große Vielfalt an Datensätzen privater Unternehmen zu sammeln, wie beispielsweise Telefondaten. Abschnitt 215 bezieht sich daher auf die Sammlung gespeicherter Daten.

Der Kongress hat 1978 den Foreign Intelligence Surveillance Act (FISA) verabschiedet und zwischen der Überwachung von US-Personen und Zielpersonen im Ausland unterschieden[119]. Die Terrorangriffe vom 11. September 2001 haben zu einer massiven Vergrößerung des nationalen Sicherheitsapparats geführt. FISA-Änderungen von 2001 und 2008 haben die Definition weiter gedehnt, welche Informationen gesammelt werden dürfen. Vor 2008 hat der FISA es nur erlaubt »Fremdmächte« oder »Vertreter von Fremdmächten« zu überwachen[120]. Seit 2008 sind NSA und andere Geheimdienste befugt, »ausländische Geheimdienstinformationen« zu sammeln, einschließlich »Informationen, die sich auf eine Fremdmacht oder ausländische Gebiete beziehen, die einen Bezug zu auswärtigen Angelegenheiten der USA besitzen«[121]. Diese Definition reicht weit über Terrorismusbekämpfung oder nationale Sicherheit hinaus, welche die

eigentlichen Ziele der Geheimdienstaktivitäten sind. Dadurch wird die Massenüberwachung ausländischer Kommunikation, die von den Snowden-Dokumenten aufgedeckt wurde, erst möglich. Zusätzlich setzt das Gesetz nur gerine Rechtsschranken bei der Informationssammlung solange sich zumindest einer der Kommunikationspartner außerhalb der USA befindet. Die Informationen, die gesammelt werden können, schließen die Metadaten von Telefongesprächen und E-Mails (z.B. Nummern, Anrufdauer, E-Mail-Adressen) ebenso wie den Inhalt der Kommunikation ein.

Die massenhafte Sammlung von Echtzeitdaten direkt auf den Leitungen verlangt eine rechtliche Unterscheidung des Abhörvorgangs und der Verarbeitung der Daten, um nach Zielen zu suchen. Massenabhörung und -sammlung von Internetverkehr wird unvermeidbar sowohl inländische als auch ausländische Kommunikation erfassen. Auch wenn das gezielte Abhören einer US-Person einen richterlichen Beschluss verlangt, wird das Datensammeln an sich noch nicht als gezielte Handlung angesehen. Die massenhaft gesammelten Daten werden gefiltert und sortiert, um Informationen zu löschen, die nicht verarbeitet werden dürfen, indem man im Grunde zwischen in- und ausländischer Kommunikation trennt. Kurz gesagt ist das Abfangen jeglichen Kommunikationsverkehrs in breitem Umfang erlaubt worden und die rechtlich erforderliche Einschränkung der Verwendung erfolgt erst nach der Sammlung.

Die durch den FISA autorisierten Überwachungsprogramme erlauben es Strafverfolgungsbehörden auch, Privatunternehmen dazu zu zwingen, Zugriff auf ihre gespeicherten, übermittelten und verarbeiteten Daten zu gewähren, die in Zusammenhang mit Geheimdienstzielen stehen könnten. Abschnitt 215 des US PATRIOT Act gewährt der Regierung auch Zugriff auf die Daten privater Unternehmen[122]. Auf Basis von Abschnitt 215 kann das FBI in Auftrag der NSA den FISA-Gerichtshof um eine Anordnung für ein US-Unternehmen ersuchen, damit dieses auslandsgeheimdienstliche Informationen im Rahmen laufender Ermittlungen bereitstellen muss. Der Anwendungsbereich von Abschnitt 215 ist sehr breit gefasst, obwohl auch hier zwischen in- und

ausländischer Kommunikation unterschieden werden muss. Daten von Personen innerhalb der USA dürfen nicht gesammelt werden, es sei denn, es finden Ermittlungen im Rahmen von internationalem Terrorismus oder illegaler Geheimdienstaktivitäten anderer Länder statt.

Ausmaß und Bedingungen der Überwachung

Die Snowden-Dokumente zeigen, dass die US-Regierung eine riesige Infrastruktur zur Unterstützung der Internetüberwachung aufgebaut hat. Die Programme, die riesige Massen an Daten sammeln, haben Zugriff auf die bedeutendsten Internet-Verbindungsknoten in den USA. Das bedeutet, dass sie jegliche Kommunikation, die in oder aus dem Land kommt, überwachen können[123]. Weil ein Teil dieser Kommunikation für den Auslandsgeheimdienst interessant sein könnte, wird jede Kommunikation an all diesen Orten überwacht. Diese Logik rechtfertigt den Zugriff der Regierung auf einen Großteil des internationalen Telekommunikationsverkehrs, der die USA passiert. In ähnlicher Weise verlangt eine Anordnung des FISA-Gerichtshofs, die von Snowden veröffentlicht wurde, auf Grundlage des US PATRIOT Act von Verizon, AT&T und Sprint, Metadaten aller Telefongespräche innerhalb der USA und zwischen den USA und anderen Staaten auf täglicher Basis bereitzustellen[124]. Diese Daten werden dann von der NSA verwahrt. Die Berechtigung galt die letzten sieben Jahre hindurch und wurde alle drei Monate vom FISA-Gerichtshof erneuert. Zu Überwachungszwecken hat die US-Regierung auch Zugriff auf Untersee-Glasfaserkabel eingerichtet – als Teil eines Pakets an Programmen (eines davon trägt den Namen »Unbeschränkter Informant«), die riesige Mengen Rohdaten abfangen, die durch das Internet laufen[125].

Aber die Aktivitäten der NSA beschränken sich nicht darauf, auf Daten zuzugreifen, die durch die Kabel privater Netzbetreiber laufen. Das mittlerweile berühmte PRISM-Programm gewährt der NSA durch ein Gerichtsurteil Zugriff auf spezifische Nutzerdaten von neun großen amerikanischen Anbietern von Internetinhalten und -diensten. Laut

dem Direktor des Inlandsgeheimdienstes (DNI) ist PRISM »ein regierungsinternes Computersystem, dass die rechtlich gestützte Sammlung auslandsgeheimdienstlicher Informationen von Kommunikationsdienstleistern ermöglicht«, das bis ins Jahr 2008 zurückgeht[126]. PRISM wird durch Abschnitt 702 des FISA autorisiert. Es konzentriert sich auf ausländische Ziele. In manchen Fällen haben sich Unternehmen der Zusammenarbeit widersetzt. Kurz nach den ersten Medienberichten gewann Yahoo ein Gerichtsverfahren am FISA-Gerichtshof, das die Veröffentlichung von NSA-Dokumenten anordnete, die den Widerstand von Yahoo gegen die Herausgabe von Kundendaten an die US-Regierung dokumentierten[127]. 2011 brachte ein geheimgehaltenes Unternehmen einen Fall vor den FISA-Gerichtshof, der urteilte, dass die NSA durch das unbefugte Durchsuchen privater Daten das Fourth Amendment verletzt hatte[128].

Die ständig aktualisierten Datenbanken mit überwachten und gespeicherten Informationen werden dann zu Geheimdienstzwecken analysiert. Das wirkungsvollste Werkzeug hierfür ist als XKeyscore bekannt. Es ist ein raffiniert durchdachtes Such-Interface, dass es einem Analysten ermöglicht, Anfragen zu stellen, die Daten aus verschiedenen anderen Programmen beziehen. Das Programm macht es möglich, riesige Datenbanken mit abgefangenem Internetverkehr zu durchsuchen. Analysten können mit Namen, Telefonnummer, IP-Adresse, Schlüsselwörtern, Browsertyp und Sprache suchen, um auf den Inhalt von E-Mails, Online-Chats und anderer Kommunikation zuzugreifen.

Diese Programme und die gesetzlichen Berechtigungen erlauben die fortlaufende Sammlung globaler Kommunikation ohne Rücksichtnahme darauf, was genau gesammelt wird. Offensichtlich bedeutet das, dass sie auch Daten abgreifen, die außerhalb der Kompetenz des Auslandsgeheimdienstes liegen. Anschließend werden auf Grund dessen, was legal gewesen wäre, diejenigen Daten ausgewählt, die behalten, analysiert und verteilt werden können. Beispielsweise muss jede Kommunikation, in die eine US-Person involviert ist, gelöscht werden.

Es sei denn, der NSA-Direktor bestätigt schriftlich, dass die Daten relevant für den Auslandsgeheimdienst sind und Anzeichen auf ein Verbrechen oder notwendige Informationen zum Verstehen oder Einschätzen einer Bedrohung von Kommunikationssicherheit enthalten oder zu Informationen gehören, die eine Bedrohung oder eine ernsthafte Schädigung von Leben oder Eigentum beinhalten. Die American Civil Liberties Union und die Electronic Frontier Foundation haben auf Grundlage von First, Fourth und Fifth Amendment vor Gericht Klagen eingereicht, um die exzessive Sammlung und den Angriff innerstaatlicher Kommunikation durch viele dieser Programme zu beenden.

Ein umfassender Überblick über alle Geheimdienstprogramme der NSA, die die Sammlung von Telefon- und Internetdaten ermöglichen, kann hier in Kürze nicht gegeben werden. Die geleakten Dokumente machen aber deutlich, dass die Überwachungskapazitäten der USA von globaler Bedeutung sind. Die NSA nutzen aus, dass ein Großteil des internationalen Datenverkehrs durch Server, die in den USA liegen und von US-Unternehmen angeboten werden, geroutet wird. Die Möglichkeiten der USA werden durch enge Zusammenarbeit mit anderen Staaten weiter vergrößert. Die USA, Großbritannien, Neuseeland, Kanada und Australien haben die »Five Eyes Alliance« begründet, um Geheimdienstinformationen auszutauschen[129]. Die Zusammenarbeit der USA mit Großbritannien scheint besonders eng zu sein, wie wir später darlegen werden. Die NSA arbeitet auch eng mit dem deutschen Geheimdienst BND zusammen, wobei nach wie vor wenig über die konkrete Form und das Ausmaß des Austauschs zwischen den beiden Ländern bekannt ist.

Aufsicht über Geheimdienste und Überwachungsprogramme

Die große Bandbreite von US-Überwachungsprogrammen bringt verschiedene Arten der Aufsicht durch verschiedene Regierungszweige mit sich. Am bekanntesten ist die richterliche Aufsicht über die größten Programme durch den FISA-Gerichtshof, der sich aus elf bundesstaatlichen Richtern zusammensetzt, die vom Obersten Richter

der USA ernannt werden. Der FISA-Gerichtshof tritt im Geheimen zusammen, erlaubt es nur der Regierung, vorzusprechen und legt dem Kongress jährlich einen Bericht über seine Tätigkeiten vor. Dadurch, dass nur sehr wenige Anträge auf Kommunikationsüberwachung vom FISA-Gericht abgelehnt werden, sprechen Kritiker von »Blanko-Scheinen« für Regierungsanfragen[130]. Dennoch ermöglicht es schon das Wesen der richterlichen Aufsicht dem FISA-Gerichtshof nicht, die Durchführung der Überwachungsprogramme zu beaufsichtigen. Die Minimierungsansätze von FISA folgen dem »Erst sammeln, dann aussortieren«-Modell. Daher wird die Verantwortung, festzustellen, ob etwas konform zu dem FISA ist, auf die Exekutive verlagert[131].

Die Geheimdienst- und Rechtsausschüsse im Senat und dem Repräsentantenhaus beaufsichtigen im Allgemeinen alle geheimdienstlichen Datensammelprogramme und die Ausschussmitglieder werden regelmäßig auf den neuesten Stand gebracht. Die Kongressmitglieder erhalten vor jeder erneuten Bewilligung einen ausführlichen Bericht. Dennoch ist es den Kongressmitgliedern untersagt, relevante Informationen an die Öffentlichkeit zu tragen und die Auffassungen des FISA-Gerichts sind geheim. Kongressmitglieder haben sich darüber beschwert, dass sie nicht ausreichend über die NSA und andere Geheimdienstaktivitäten informiert sind, um wirksame Aufsicht leisten zu können[132].

Andere Methoden zur Durchsetzung der Rechenschaftspflicht existieren und sind speziellen Bewilligungsgesetzen zugeordnet. Zum Beispiel beinhaltet die Aufsichtshoheit aus Abschnitt 215 des US PATRIOT Act alle drei Regierungszweige und besteht aus (1) einem halbjährlichen Bericht an den Kongress, (2) einem Treffen von Justizministerium, Mitarbeitern des Direktors der nationalen Nachrichtendienste und der NSA, das zumindest alle 90 Tage stattindet und (3) einem Bericht, der dem FISA-Gericht alle 30 Tage vorgelegt werden muss. Auslandsüberwachung wird von Exekutive, Judikative und Legislative der US-Regierung weniger streng beaufsichtigt. Hier besteht die Aufsicht aus (1) einen jährlichen Bericht des NSA-Generalinspekteurs,

(2) einen halbjährlichen Bericht an den FISA-Gerichtshof und den Kongress über die Durchführung der Programme, (3) einen halbjährlichen Bericht an den FISA-Gerichtshof und den Kongress über die Konformität mit dem Generalstaatsanwalt und dem DNI und einen (4) vierteljährlichen Bericht an den FISA-Gerichtshof über die Rechtsbefolgung. Innerhalb der Exekutive muss die NSA dem Justizministerium und den Mitarbeitern des DNI Bericht über jeden Fall von Verletzung des FISA Gesetzes erstatten, sowie über jede gezielte Überwachung von in den USA befindlichen Personen, die fälschlicherweise außerhalb der USA vermutet wurden. Letztlich gibt es nun eine neue und bisher unerprobte Aufsichtsinstanz, das Privacy and Civil Liberties Oversight Board (PLCOB), das sich nun mit einer Überprüfung der NSA-Überwachungsaktiväten beschäftigt.

Großbritannien

Rechtliche Autorisierung

Der Intelligence Services Act (ISA) von 1994 und der Regulation of Investigatory Powers Act (RIPA) von 2000 formen den rechtlichen Rahmen für Government Communication Headquarters (GCHQ), den britischen Geheimdienst, der für den Abfang von Nachrichtensignalen und die Informationssicherung zuständig ist. ISA autorisiert die Arbeit der Geheimdienste zu Zwecken der nationalen Sicherheit und Außenpolitik, für wirtschaftliche Interessen und zur Vorbeugung oder Erkennung schwerwiegender Straftaten. GCHQ steht unter Aufsicht des Außenministeriums. Der Direktor von GCHQ ist dafür verantwortlich, dass »GCHQ keine Informationen erhält, die es nicht zur ordnungsgemäßen Erfüllung seiner Funktion benötigt.« GCHQ und andere Geheimdienstbehörden wie der Security Service (MI5) und der Secret Intelligence Service (MI6) müssen sich eine Anordnung eines Ministers einholen, um Telekommunikationsüberwachung durchführen zu dürfen. Der zuständige Minister entscheidet, ob die beantragte Überwachung im Kompetenzbereich der Geheimdienste liegt.

RIPA regelt eine große Bandbreite an Überwachungsaktivitäten von Strafverfolgungsbehörden und Geheimdiensten. RIPA ordnet die

Zusammenarbeit und das Bereitstellen von Abhörschnittstellen von Telekommunikationsbetreibern für bewilligte Überwachungsprogramme an[133]. Überwachungsanordnungen eines Ministeriums müssen für den geheimdienstlichen Zweck angemessen und notwendig sein, wie oben bereits ausgeführt. Anordnungen müssen geheimgehalten und alle sechs Monate erneuert werden. Eine Anordnung kann sich entweder auf eine Person beziehen oder auf eine Reihe von Örtlichkeiten. Beispielsweise könnte ein Büro als Ort ein Ziel sein, womit jede Kommunikation von diesem und zu diesem Ort überwacht werden würde. Der Begriff »Schutzmaßnahmen« lässt viel Raum für Interpretationen durch die Geheimdienste. RIPA erfordert es, so wenigen Personen wie möglich Datenzugriff zu gewähren und das Ausmaß der Offenlegung sowie die Anzahl der Vervielfältigungen zu minimieren. Für das Abhören ausländischer Kommunikation braucht es keine genaue Beschreibung der Zielpersonen oder -orte[134].

Ausgehend von den durch Snowden veröffentlichten Dokumenten dient RIPA als rechtliche Grundlage für das Anzapfen von Glasfaserleitungen. GCHQ beruft sich auf Abschnitt 8, Paragraph 4 von RIPA, um Anordnungen für außerbritische Kommunikationsüberwachung zu beantragen[135]. Das erlaubt der Behörde, externe Kommunikation mitzuhören bei der sich zum Beispiel eine der Zielpersonen außerhalb Großbritanniens befindet. In den meisten Fällen in RIPA muss einem Minister der Name einer Zielperson oder eines Unternehmens bekannt sein, bevor die Anordnung ausgestellt wird. Aber Abschnitt 8 erlaubt es GCHQ, wahllos externe Daten abzugreifen, wenn der Minister zusammen mit der Anordnung ein »Zertifikat« ausstellt. Laut dem, was die Dokumente besagen, berechtigen diese Zertifikate GCHQ, unter einer Vielzahl von Vorwänden nach Material zu suchen: Aufklärung über die politischen Absichten fremder Regierungen; die militärische Haltung fremder Staaten; Terrorismus; internationaler Drogenhandel und Betrug. Wie berichtet wird, gibt es »10 Basiszertifikate, darunter ein»globales«, dass die Versorgungsstationen der Behörde in Bude in Cornwall, Menwith Hill in North Yorkshire und Zypern einschließt«[136].

Ausmaß und Bedingungen der Überwachung

Die Struktur und Funktionalität der britischen Überwachungsprogramme scheinen ähnlich zu denen der USA und beinahe genauso breit angelegt. Durch die geographische Lage des UK, treffen dort eine Vielzahl von Untersee-Glasfaserkabeln zusammen, die Internetverkehr transportieren, bevor dieser den Atlantik überquert. Der *Guardian* berichtete, dass im Sommer 2001 GCHQ Abhörsonden an mehr als 200 dieser Kabel angebracht hatte, um Daten zu Geheimdienstzwecken zu filtern und zu speichern[137]. Dieses Programm mit dem Codenamen Tempora ist Teil zweier Projekte, die den Titel »Mastering the Internet« und »Global Telecoms Exploitation« tragen, was die Ambitionen von GCHQ reflektiert, das gesamte Internet zu überwachen. Als Mitglied des »Five Eyes«-Geheimdienstzusammenschlusses, einer Allianz bestehend aus USA, Kanada, Großbritannien, Neuseeland und Australien, arbeitet Großbritannien eng mit der NSA zusammen, um Geheiminformationenn zu sammeln und auszutauschen. Der *Guardian* zitiert geleakte Dokumente, die besagen, dass »GCHQ und NSA es vermeiden, die selben Daten zweimal zu verarbeiten und aktiv versuchen, technische Lösungen und Verarbeitungsarchitekturen zu vereinen«[138]. Zurzeit sind 300 Analysten von GCHQ und 250 der NSA direkt damit beauftragt, das gesammelte Material zu untersuchen. Im Herbst 2011 wurde der NSA voller Zugriff gewährt. Eine Schlüsselfrage (die wir bisher nicht durch unsere Nachforschungen beantworten konnten) ist, wie inländische Kommunikation, die unbeabsichtigt zusammen mit ausländischer Kommunikation abgefangen wurde, von den britischen Geheimdiensten behandelt wird.

Die Zusammenarbeit von NSA und GCHQ scheint weit über das Tempora-Programm hinauszugehen. Laut Berichten des *Guardian* hat die NSA GCHQ 100 Millionen Pfund für Überwachungsprogramme gezahlt[139]. Anscheinend haben britische Geheimdienstvertreter niedrige Datenschutzstandards und eine großzügige Rechtsaufsicht als Verkaufsargumente gegenüber NSA-Vertretern benutzt. Finanzierung

durch die NSA scheint eine wichtige Einkommensquelle für GCHQ zu sein und gewährt US-Geheimdienstlern nicht nur Zugriff auf britische Programme, sondern erlaubt ihnen auch, diese zu beeinflussen. Weitere aktuelle Berichte decken auf, dass NSA und GCHQ auch bei der Kompromittierung verbreiteter Verschlüsselungsstandards für Internetkommunikation zusammenarbeiten[140].

GCHQ verfügt auch über Programme, die britische Anbieter von Internetzugängen, -inhaltne oder -diensten zur Kooperation zwingen. Die (gelöscht deutsche Zeitung) *Süddeutsche Zeitung* berichtete, dass GCHQ eng mit dem Telekommunikationsanbietern British Telecom, Verizon, Vodafone, Global Crossing, Level 3, Viatel und Interroute zusammenarbeitet, um nicht nur Zugriff auf die Kommunikationswerke zu erhalten, sondern auch um Überwachungsprogramme und -software zu entwickeln[141].

Aufsicht über Geheimdienste und Überwachungsprogramme

Entsprechend des ISA muss der Direktor von GCHQ jedes Jahr einen Bericht für den Premierminister und den zuständigen Minister anfertigen. Außerdem stellt der Interception of Communications Commissioner (ICC) sicher, dass Regierungsbehörden beim Abhören von Kommunikation entsprechend ihrer rechtlichen Verantwortung handeln[142]. Der Commissioner bewertet auch die Rolle des zuständigen Ministers beim Ausstellen von Abhöranordnungen. Der ICC scheint jedoch nur einen kleinen Teil der Anordnungen zu überprüfen und dann auch nur, nachdem sie vom Ministerium bereits ausgestellt wurden[143]. Stellt der ICC ein Fehlverhalten fest, muss das dem Premierminister gemeldet werden, aber eine Veröffentlichungspflicht besteht nicht. Daher liegen Bewilligungen und Überprüfung vollständig in Händen der Exekutive.

Das Investigatory Powers Tribunal, das sich aus neun erfahrenen Anwälten zusammensetzt, nimmt Beschwerden von Einzelpersonen entgegen, die meinen, unrechtmäßig überwacht worden zu sein[144]. Das

Tribunal kann aber keine eigenen Ermittlungen initiieren. Menschen außerhalb der Geheimdienste erfahren kaum von den Verfehlungen und können so auch keine Beschwerde einreichen. Darüberhinaus unterliegt das Tribunal aus Gründen öffentlicher oder nationaler Interessen strengen Geheimhaltungsvorschriften.

Der Geheimdienst- und Sicherheitsausschuss des Parlaments (ISC) beaufsichtigt die UK-Geheimdienste, einschließlich ihrer Ausgaben, Verwaltung und Handlungsgrundlagen[145]. Der Ausschuss veröffentlicht jährlich einen Bericht. Der letzte Bericht für 2012/2013 konzentriert sich auf die Leistung, Effektivität und das Budget der Geheimdienstbehörden. Er untersucht nicht deren Einfluss auf bürgerliche Freiheiten, Privatsphäre oder Datenschutz. Am 17. Juli veröffentlichte das ISC eine Stellungnahme zu den Abhörmaßnahmen von GCHQ unter dem PRISM-Programm[146]. Nachdem er »detaillierte Beweise von GCHQ« erhalten hatte, kam der Ausschuss zu dem Schluss, dass Behauptungen unrechtmäßiger Datensammlung durch GCHQ haltlos seien. Der Ausschuss gab jedoch auch bekannt, eine Untersuchung des »komplexen Zusammenwirkens von Intelligence Services Act, Human Rights Act und RIPA« durchzuführen, sowie »der Leitlinien und Verfahren, die diese untermauern.« Diese Überprüfung ist bisher noch nicht zu einem öffentlich bekannten Abschluss gekommen.

Die britischen Überwachungsprogramme unterliegen keiner starken richterlichen Kontrolle. Die Befugnisse aus RIPA brauchen generell keinerlei richterliche Erlaubnis und können für eine Vielzahl an Zwecken herangezogen werden. Während der Posten des Commissioners mit einem ehemaligen Richter des Obersten Gerichtshofs besetzt ist, glauben Kritiker der aktuellen Überwachungsherrschaft, dass richterliche Einwilligung die bestmögliche Verbesserung des momentanen Systems bedeuten würde[147]. Insgesamt ist die Aufsicht über die britischen Überwachungsprogramme sehr limitiert. Es scheint nur sehr begrenzte gesetzgeberische und keinerlei richterliche Kontrolle zu geben. Es ist nur wenig über die Minimierungsprozesse

bekannt, die GCHQ zur Zugriffsbeschränkung oder Löschung der Daten benutzt, die unrechtmäßig gesammelt wurden. Privacy International hat angekündigt, dass sie in Erwägung ziehen, die Rechtmäßigkeit von Tempora und der Zusammenarbeit von GCHQ und Internet Service Providern vor Gericht in Frage zu stellen[148].

Deutschland

Rechtliche Autorisierung

Der Bundesnachrichtendienst (BND) arbeitet auf Basis eines Gesetzes, dass 1990 vom Bundestag verabschiedet wurde[149]. §1, Absatz 2 des BND-Gesetztes erlaubt es dem BND, Informationen aus dem Ausland zu ermitteln, die relevant für die deutsche Außenpolitik oder nationale Sicherheit sind. Das Gesetz verlangt eine strikte Trennung des Geheimdienstes von Polizei und Strafverfolgung. §2, Absatz 4 verpflichtet den BND, Geheimdienstinformationen mit denjenigen Methoden zu sammeln, die für die Zielperson am wenigsten Störungen verursachen. Es muss auch eine Balance zwischen den negativen Konsequenzen der Überwachung und dem anvisierten Informationsgewinn bestehen. Wie die Wortwahl oben bereits andeutet, ist das Gesetz so weit gefasst, dass es wenig konkrete Orientierungspunkte für die rechtlichen Grenzen von Überwachungsprogrammen liefert. Das Gesetz erlaubt es dem BND außerdem, nach §1, Absatz 2, Daten von Telekommunikationsanbietern anzufragen.

Während der BND über ein weitreichendes Mandat verfügt, auslandgeheimdienstliche Informationen zu sammeln, wenn diese der deutschen Außenpolitik und dem nationalen Sicherheitsinteresse dienen, sind alle Aktivitäten, die mit dem Artikel 10 des Grundgesetzes (Brief-, Post- und Fernmeldegeheimnis) in Konflikt geraten, Gegenstand des G10-Gesetzes und benötigen die Zustimmung der G10-Kommission (siehe unten). Das gilt für alle deutschen Nachrichtendienste, inklusive BND, Militärischer Abschirmdienst (MAD) und Bundesamt für Verfassungsschutz. Das G10-Gesetz definiert die Ziele einer

Autorisierung von Programmen zur Überwachung internationaler Kommunikation näher. Als legitime Rechtfertigung für eine solche Überwachung führt es unter anderem die Gefahr eines bewaffneten Angriffs auf Deutschland, die Gefahr (gelöscht) internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik und die Gefahr der internationalen Verbreitung von Kriegswaffen auf. Aber der Auftrag ist immernoch breit definiert. Er umfasst auch Drogenhandel, internationale Geldwäsche und Menschenhandel.

Unter Rechtswissenschafltern ist umstritten, ob Artikel 10 des Grundgesetzes auch die Kommunikation zwischen Ausländern außerhalb Deutschlands schützt und das G10-Gesetz sie dadurch auch betrifft[150]. Der Richter Berthold Huber, der auch Mitglied der G10-Kommission ist, schrieb in einem kürzlich in einem rechtswissenschaftlichen Journal erschienenen Artikel, dass die Regierung außerdeutsche Kommunikation als nicht von Artikel 10 gedeckt und damit nicht unter das G10-Gesetz und die Aufsicht der G10-Kommission fallend betrachtet[151]. Niko Härting meint, dass der BND sich nur den Datenschutzgesetzen unterwerfen muss, wenn er innerhalb Deutschlands tätig ist[152]. Das sind nicht die einzigen kontroversen Punkte. Härting führt auch an, dass die gegenwärtige Rechtslage dem BND die Sammlung von Metadaten nicht erlaubt[153].

Laut BND-Gesetz ist es dem BND gestattet, personenbezogene Daten gemäß seines Auftrags zu sammeln, zu speichern, zu ändern und zu analysieren. Die Schaffung neuer Datenbanken mit personenbezogenen Daten muss vom Kanzleramt genehmigt werden. Dabei gelten die Datenschutzbestimmungen des Bundesamts für Verfassungsschutz. Daten, die für den angegebenen Zweck nicht mehr benötigt werden oder durch nicht genehmigte Methoden eingeholt wurden, müssen gelöscht werden. Die Datenschutzbestimmungen des G10-Gesetzes sind strenger. §5 verbietet das Einholen von Daten aus dem »Kernbereich privater Lebensgestaltung«. §6 verpflichtet die Nachrichtendienste, regelmäßig zu überprüfen, ob die gesammelten Daten noch für die genehmigten Zwecke benötigt werden. Diese Prüfung ist einmal nach dem Erhalt der

Daten und anschließend alle sechs Monate durchzuführen. Wenn die Daten nicht mehr benötigt werden, müssen sie unverzüglich gelöscht werden. Die Löschung muss dokumentiert werden. Das Gesetz limitiert streng, wie und unter welchen Bedingungen Daten, die gemäß des G10-Gesetzes eingeholt wurden, mit anderen Regierungsbehörden oder ausländischen Nachrichtendiensten geteilt werden dürfen. Die Struktur des Nachrichtenbeschaffungssystems ist ähnlich wie in Großbritannien und den Vereinigten Staaten. Das Gesetz erlaubt weitgehende Nachrichtenbeschaffung, wenn diese den Bedürfnissen und Interessen der Auslandsaufklärung dient. Die Einschränkungen und Minimierungserfordernisse, die man in Deutschland eventuell als strenger ansehen kann, werden erst angewendet, wenn die ursprüngliche Überwachung bereits stattgefunden hat.

Ausmaß und Bedingungen der Überwachung

Über einzelne Überwachungsprogramme des BND ist nur sehr wenig bekannt. Medienberichten zufolge überwacht der BND routinemäßig internationale Telekommunikationsvorgänge an Deutschlands größtem Internet-Knoten DE-CIX in Frankfurt am Main[154]. Die Befugnis für diese Überwachungsmaßnahme begründet sich aus dem G10-Gesetz (§5 und 10, Abschnitt 4). Dort heißt es, dass die Überwachung von internationalen Telekommunikationsbeziehungen für genehmigte, grob definierte Zwecke durchgeführt werden kann, aber nur 20% der »Übertragungskapazität« genutzt werden dürfen. Was mit »Übertragungskapazität« genau gemeint ist und wie dieser Wert die Überwachungsprogramme des BND einschränkt, ist unklar. Eine Definition, die auf Kapazität basiert, erlaubt dem BND einen viel weitreichenderen Zugriff auf Internet-Daten als die für gewöhnlich in der Presse angeführten 20% des Datenverkehrs.

Das Parlamentarische Kontrollgremium (PKGr) erstellt jedes Jahr einen kurzen, allgemein gehaltenen Bericht zu den Überwachungsmaßnahmen. Dem Bericht für das Jahr 2010 wurde größere Aufmerksamkeit der Medien zuteil, weil aus ihm hervorging, dass automatisierte Suchen mit mehr als 15.000 Zielbegriffen mehr als

37 Millionen Kommunikationsvorgänge, hauptsächlich eMails, zur genaueren Untersuchung identifiziert hatten[155]. Letztendlich wurden 213 dieser Kommunikationsvorgänge als relevant angesehen und abgespeichert. Der Bericht liefert weitere Anhaltspunkte dafür, dass der BND den Internetverkehr in großem Maßstab filtert[156]. Der BND gibt an, dass die große Zahl eingefangener Kommunikationsvorgänge das Ergebnis eines ungewöhnlich hohen Spam-Mail-Aufkommens war. Der Bericht für das Jahr 2011 weist nur noch 3 Millionen eingefangene Kommunikationsvorgänge aus[157].

Da die Anzahl der Suchbegriffe nur leicht sank, ist die wahrscheinlichste Erklärung für die geringere Trefferzahl die Verbesserung der automatischen Filtermechanismen[158]. Die Partei Die Linke nutzte eine parlamentarische Anfrage, um mehr über die BND-Überwachung der Telekommunikation zu erfahren. Die Antwort des Kanzleramts bestätigte, dass der BND automatisierte Durchsuchungen der Internetkommunikation vornimmt. Der Bericht enthält nur sehr wenige Informationen zum Umfang der Programme und den Minimierungsprozessen. Diese Informationen bleiben unter Verschluss, da sie nach Angaben des BND Aufschluss über Methoden und Leistungsfähigkeit des BND geben könnten und damit die deutsche Regierung in ihren Bemühungen hindern könnten, das Land zu schützen. Allerdings heißt es, dass nach dem automatisierten Filterungsprozess mehrere Evaluations- und Bewertungsverfahren durch Analysten sicherstellen sollen, dass nur Daten, die für die Ziele des BND relevant sind, für weitere Analysen gespeichert werden. Alle anderen Daten sollten gelöscht werden.

Deutsche Nachrichtendienste haben starke historische Verknüpfungen mit US-Nachrichtendiensten, die auf die enge Zusammenarbeit während des Kalten Krieges zurückzuführen sind[159]. Es ist allgemein bekannt, dass die NSA und andere amerikanische Nachrichtendienste über Anlagen und Mitarbeiter auf US-Militärbasen in Deutschland verfügen. Nach den Anschlägen vom 11. September wurde die Zusammenarbeit

zwischen deutschen und amerikanischen Nachrichtendiensten weiter ausgebaut. Dokumente, die von Edward Snowden geleakt wurden, geben Einblick in die Art der engen Kooperation. Vertreter der Vereinigten Staaten behaupten, der BND-Präsident habe bei der deutschen Regierung für eine rechtliche Interpretation der Datenschutzbestimmungen geworben, die den Datenaustausch mit amerikanischen Nachrichtendiensten erleichtern würde[160]. Der SPIEGEL berichtet von gewaltigen Mengen an Metadaten, die der BND regelmäßig an die NSA übermittelt[161]. Der BND behauptet, diese Daten stammen aus ausländischen Kommunikationsvorgängen und alle Daten, die deutsche Bürger betreffen, würden entfernt. Die Dokumente zeigen auch, dass der BND das XKeyscore-System der NSA benutzt, das einem Analysten Zugang zu allen Telekommunikationskanälen einer Zielperson geben soll.

Aufsicht über Geheimdienste und Überwachungsprogramme

Das Parlamentarische Kontrollgremium führt die gesetzliche Aufsicht über die Nachrichtendienste. Das Kanzleramt ist verpflichtet, das PKGr regelmäßig (mindestens einmal in sechs Monaten) über die Aktivitäten der Nachrichtendienste zu informieren. Das PKGr kann Dokumente und Daten anfordern und Anhörungen mit Mitarbeitern der Nachrichtendienste durchführen. Die Inhalte der Beratungen des PKGr werden geheim gehalten, können allerdings mit einer Zweidrittelmehrheit öffentlich gemacht werden. Das Gremium erstellt jedes Jahr einen Bericht, der die Gesamtzahl der Informationsanfragen und die Zahlen für jeden einzelnen Nachrichtendienst sowie die Art der nachgefragten Informationen enthält.

Außerdem ernennt das PKGr die vier Mitglieder und die vier stellvertretenden Mitglieder der G10-Kommission, die als ständiges Aufsichtsorgan für nachrichtendienstliche Aktivitäten dient. Die Kommission überprüft und autorisiert alle Anfragen für Überwachungsmaßnahmen die unter das G10-Gesetz fallen[162]. Der Vorsitzende der G10-Kommission muss die Befähigung zum Richteramt

haben. Die Kommission kommt mindestens einmal im Monat zusammen und kann »Kontrollbesuche« von Anlagen deutscher Nachrichtendienste vor Ort durchführen. Die G10-Kommission kann nicht nur Überwachungsprogramme autorisieren, sondern auch ihre Durchführung bezüglich Sammlung, Speicherung und Analyse persönlicher Daten kontrollieren. Die Nachrichtendienste müssen ihre Überwachungsanfragen rechtfertigen und deren Umfang sowie ihre Ziele spezifizieren. Die Kommission erhält auch die Bürgerbeschwerden und untersucht möglichen Missbrauch. Da die Aufsichtsorgane in Deutschland in der Zuständigkeit des Bundestags sind und damit der Legislative zuzurechnen sind, enthalten die Aufsichtsmaßnahmen keine gerichtliche Überprüfung.

Andere Aufsichts-Maßnahmen werden von Institutionen der Exekutive ausgeübt. Der BND muss dem Kanzleramt Bericht erstatten. Das Kanzleramt, das Innenministerium (dem das Bundesamt für Verfassungsschutz Bericht unterstellt ist) und das Verteidigungsministerium (dem der Militärische Abschirmdienst unterstellt ist) müssen dem Parlamentarischen Kontrollgremium mindestens alle sechs Monate über die Aktivitäten der deutschen Nachrichtendienste informieren. Nach dem G10-Gesetz braucht der BND die Zustimmung des Kanzleramts, um nach diesem Gesetz gesammelte Informationen mit Nachrichtendiensten anderer Länder zu teilen.

Bürgerinnen und Bürger, die annehmen, dass sie überwacht wurden, können vom BND die Herausgabe von ihnen betreffenden Informationen verlangen[163]. Die Anfrage muss eine Erklärung enthalten, warum der Bürger davon ausgeht, überwacht worden zu sein, und ein besonderes Interesse in der Offenlegung dieser Informationen erkennen lassen. Der BND kann die Anfrage zurückweisen, wenn die Offenlegung seine Aufgabenerfüllung, seine Quellen oder die öffentliche Sicherheit gefährden könnte.

Deutsche Datenschutzbeauftragte haben die deutsche Regierung öffentlich für ihre Weigerung, die Reichweite der Überwachung deutscher Bürgerinnen und Bürger durch deutsche und ausländische Geheimdienste zu untersuchen, kritisiert. Sie riefen zu einer Reform der

Aufsichtsmechanismen auf, um die deutschen Überwachungsprogramme unter bessere Kontrolle zu stellen[164]. Außerdem hätten sie gerne ihren Aufgabenbereich bei der Untersuchung von Datenschutzvorgängen auf Daten, die nach dem G10-Gesetz gesammelt wurden, ausgeweitet.

Ergebnisse

Obwohl wir nicht über alle relevanten Fakten jedes Falls verfügen und sozusagen nicht nur »Äpfel mit Äpfeln« vergleichen, zeigt diese Analyse, dass jedes der drei untersuchten Länder grundsätzlich einen ähnlichen Ansatz bei der Sammlung von Informationen aus Telekommunikationsnetzen verfolgt. Wenn diese Hypothese zutrifft, dürften kommende Enthüllungen zwar weitere Details zu den Überwachungsprogrammen liefern. Große neue Erkenntnisse zum rechtlichen Rahmen wären dann aber nicht zu erwarten. Zum jetzigen Zeitpunkt können wir die folgenden Schlussfolgerungen ziehen:

Rechtliche Autorisierung

In jedem der Länder sind die Gesetze, die die auf ausländische Kommunikation zielenden Programme autorisieren, unscharf formuliert und erlauben den Nachrichtendiensten, bei der Verfolgung ihrer Ziele sehr verschwiegen vorzugehen. Bei der Inlandsüberwachung sind die Standards deutlich höher. Allerdings fängt jedes Land eine Mischung aus inländischen und ausländischen Kommunikationsdaten ab. Durch die Schwierigkeiten, in Echtzeit inländische und ausländischen Daten zu unterscheiden und zu filtern, werden die Minimalisierungsmaßnahmen (etwa die Beschränkungen, was Zugang und Verwendung der gesammelten Daten betrifft) oft erst nach dem Abfangen und Sammeln durchgeführt. Das bedeutet, dass der Vorgang des Abfangens oder Überwachens unabhängig vom Ursprung und dem Inhalt der Kommunikation genehmigt wird. Es ist die Zielauswahl oder Suche im entstandenen Datenbestand und die Weiterverbreitung dieser Daten, die rechtlich beschränkt und überwacht wird. Die Logik hinter diesen Minimierungsmaßnahmen als eine Form sinnhafter Kontrolle ist zirkulär. Die Datensammler fangen alle Kommunikationsvorgänge eines

Netzwerks ab, weil ein winziger Bruchteil für die Auslandsaufklärung relevant ist. Wenn sich einige Kommunikationsvorgänge später als geschützt herausstellen, etwa weil ein eigener Bürger involviert ist, werden sie gelöscht – aber nur wenn sie keine Informationen enthalten, die für die Auslandsaufklärung relevant sind. In anderen Worten: Alle Kommunikationsvorgänge, die aus dem Internet zusammengekehrt werden und für die Auslandsaufklärung von Bedeutung sind, werden behalten und weitergegeben, egal welches rechtliche Regelwerk ihre Sammlung regulieren sollte.

Ausmaß und Umstände

Jede Regierung strebt danach, große Mengen an Daten abzufangen, die über Telefon- und Internetnetze geleitet werden – entweder durch Nutzung der eigenen Möglichkeiten oder in Zusammenarbeit miteinander. Die Geheimdienste der jeweiligen Länder scheinen alle ähnliche Werkzeuge zu verwenden, um Information für ihre geheimdienstlichen Ziele zu finden, analysieren und operationalisieren. Verfügbare Hinweise deuten darauf hin, dass die Geheimdienste von Verbündeten, wie des UK und Deutschlands, gewillt sind, mit den USA zu kooperieren, um Zugriff auf deren mächtige Geheimdienstwerkzeuge zu erlangen. Das Verhältnis von Großbritannien zu den USA ist besonders eng. Als Mitglied des »Five Eyes«-Geheimdienstzusammenschlusses genießt Großbritannien privilegierten Zugang zu US-Geheimoperationen und arbeitet eng mit den amerikanischen Geheimdienstbehörden zusammen. Außerdem erhält GCHQ direkte finanzielle Unterstützung von der NSA. Der deutsche Auslandsgeheimdienst BND hat zwar ebenfalls eine starke Verbindung zur NSA, die bis in den Kalten Krieg zurückreicht und für die globale Antiterrorbekämpfung erneuert wurde. Die genaue Beschaffenheit und das Ausmaß dieser Verbindung ist jedoch nach wie vor unklar. Länderübergreifende Geheimdienstkooperationen machen es zudem möglich, Zugriff auf inländische Kommunikation zu erhalten, deren Überwachung und Verarbeitung eigentlich für die Geheimdienstbehörden der jeweiligen Länder nicht autorisiert ist.

Aufsicht

Prüfung und Rechenschaftspflicht für diese Überwachungsprogramme ist in allen Fällen begrenzt. Jede Regierung übt direkte exekutive Aufsicht und fordert Berichtserstattung. Das britische System ist das nachlässigste, da weder Gerichte noch die Legislative ernstlich involviert sind. Nur in den USA ist ein gewisser Grad an Aufsicht durch Gerichte erforderlich, auch wenn diese nur selten Geheimdienstanfragen anfechten. Bloß in Deutschland autorisiert die Aufsichtsbehörde nicht nur die Programme, sondern trägt auch die Verantwortung für deren Durchführung und hat (gelöscht die) Untersuchungsbefugnisse. Der FISA-Gerichtshof und die G10-Kommission arbeiten in einem sehr ähnlichen Bereich, auch wenn sie in unterschiedlichen Regierungszweigen angesiedelt sind. Die Hauptverantwortung liegt darin, Regierungsanfragen nach Überwachung aus Gründen der nationalen Sicherheit gegenüber den Grundrechten von Bürgern des jeweiligen Landes abzuwägen. Aber in keinem der untersuchten Länder scheint es eine Form von Aufsicht zu geben, die der Ausweitung der Programme einen wirklichen Riegel vorschiebt. Und in allen Fällen ist das Vorgehen der Aufsichtsbehörden beinahe vollständig geheim und die Ergebnisse interner Konflikte über Vorgehen und Durchführung bleiben unbekannt.

Schlussfolgerung

Edward Snowden hat den Vorhang geöffnet, hinter dem sich die massiven Internetüberwachungsprogramme westlicher Geheimdienstbehörden verborgen haben. Medien, Regierungsvertreter, Zivilgesellschaft und Unternehmen auf der ganzen Welt stehen vor der großen Herausforderung, deren Auswirkungen zu erfassen und die Folgen abzuschätzen. (gelöscht)

Das weltweite Internet ist auf einem recht fragilen System gebaut, das aus gemeinsamer technischer Verwaltung und gegenseitiger Verpflichtung zwischen den Ländern besteht, einen offenen Markt für Ideen und Geschäfte zu erhalten – trotz der Risiken, die sich durch die offene Kommunikation für Privatsphäre und Sicherheit ergeben. Es ist ein System, das auf Vertrauen basiert. Die Snowden-Enthüllungen haben diesem Vertrauen einen erheblichen Stoß versetzt. Wenn das Vertrauen

zu stark sinkt, werden Märkte und Informationsflüsse im Internet unterbrochen werden. Nationalregierungen werden einen von Eigeninteresse geleiteten Weg einschlagen und die globale Ressource in ein System nationaler Netzwerke zergliedern, die durch nationale Interessen bewacht und beschränkt werden. Nur Wenige wünschen sich so ein Ergebnis; aber noch Wenigere haben konkrete Ideen vorgelegt, wie das verhindert werden kann. Ironischerweise ist der wahrscheinlichste Ausgang sowohl für die Ziele der Geheimdienste (die das allgemeine Vertrauen in das Internet zerschlagen haben) als auch für die Ziele Edward Snowdens (der bekundet, das freie und offene Internet zu schützen) die Unterwanderung derselben.

Die Möglichkeiten der Überwachungstechnologie sind in vielen Ländern weit über das hinausgewachsen, was die zugrundeliegenden Gesetze voraussehen hätten können und was die heutigen rechtlichen Rahmenbedingungen abdecken. Um dieses Problem anzugehen, benötigt man eine nationale Diskussion über die Aktualisierung der Gesetze, um die Balance zwischen Sicherheit und Freiheit in Übereinkunft mit nationalen Werten wiederherzustellen. Aber da das Internet ein globales System ist, beeinflusst das politische Vorgehen in einem Land die Menschen in den anderen. Wenn das Vertrauen in die Grundprinzipien des Internets wiederhergestellt werden soll, benötigt es daher einen internationalen Standardisierungsprozess für Sanktionen gegen unrechtmäßige Überwachung und die Anpassung nationaler Richtlinien an internationale Standards. Die Lösung benötigt weitaus mehr als eine Reform in Washington. Wir müssen auch über unsere eigenen Standards in Deutschland diskutieren und wie wir diese in internationale Normen gießen können. Dieser Bericht soll hierzu einen ersten Beitrag leisten.

Dieser Text ist als Studie für das Programm »Europäische Digital Agenda« der stiftung neue verantwortung und des Open Technology Institute im September 2013 erschienen[165] *und wurde für dieses Buch ins Deutsche übersetzt.*

Über das Programm Europäische Digitale Agenda: Das Potenzial des Internets als treibende Kraft für wirtschaftliches Wachstum, politischen Pluralismus und gesellschaftlichen Fortschritt ist unbestritten. Aber die Macht des Internets stellt es auch zunehmend in den Mittelpunkt von politischen, sozialen und wirtschaftlichen Auseinandersetzungen. Europa wird eine zentrale

Rolle im Kampf um die Zukunft des Internets spielen. Es mangelt allerdings an Visionen und konkreten Handlungsempfehlungen, um das große Potenzial der digitalen Revolution für das Allgemeinwohl nutzbar machen zu können. Das Programm Europäische Digitale Agenda versteht sich daher nicht nur als ein Inkubator für neue, innovative, politische Ideen, sondern möchte diese auch aktiv in die politische Debatte einbringen.

Über das *Open Technology Institute:* Das neue amerikanische Open Technology Institute unterstützt politische und regulatorische Reformen, um offene Architekturen und Open Source Innovationen zu fördern und unterstützt die Umsetzung offener Technologien und Kommunikationsnetze. OTI bewirbt erschwingliche, universelle und allgegenwärtige Kommunikationsnetze durch Partnerschaften mit Verbänden, Wissenschaftlern, der Industrie und öffentlichen Interessensgruppen und widmet sich der Aufgabe, das Potential innovativer, offener Technologien voll auszunutzen, indem sie deren sozialen und wirtschaftlichen Einfluss untersucht – vor allem für arme, ländliche und andere unterrepräsentierte Bezirke. OTI führt hierfür tiefgehende, objektive Analysen und Studien für politische Entscheidungsträger und die breite Öffentlichkeit durch.

Über *stiftung neue verantwortung:* stiftung neue verantwortung ist ein unabhängiger, non-profit und überparteilicher Think Tank in Berlin. Er fördert interdisziplinäres und bereichsübergreifendes Nachdenken über die wichtigen gesellschaftlichen und politischen Herausforderungen unserer Zeit. Durch seine Fellow- und Associate-Programme werden junge Fachleute und Vordenker aus Politik und Verwaltung, Wirtschaft, Forschung und Zivilgesellschaft zusammengebracht, um kreative Ideen und Lösungen zu entwickeln und diese durch vielfältige Veröffentlichungen und Veranstaltungen in den öffentlichen Diskurs einzubringen.

Der Koloss, der unsere Grundrechte zertrampelt, heißt NSA und es ist Zeit ihn zu bändigen

Yochai Benkler

Es ist Zeit, das NSA-Ungetüm zu zähmen, das auf unseren Grundrechten herumtrampelt. Aufgrund von Leaks und FISA-Gerichtspapieren ist es offensichtlich, dass die NSA eine aufgedunsene Bespitzelungsmaschinerie ist, die außer Kontrolle geriet. Sie kann nicht von Innen reformiert werden.

Seit der Welle an neuen NSA-Veröffentlichungen steht in der Debatte erheblich mehr auf dem Spiel. Wir wissen nun, dass die Geheimdienstbehörden systematisch die Aufsicht über sich untergraben haben, indem sie sowohl den Kongress als auch die Gerichte angelogen haben. Wir wissen, dass die NSA-Prozesse zur Standarddefinierung von Sicherheitsprotokollen des Internets, die Überwachung erschweren, infiltrierten. Wir wissen, dass die NSA durch Überredung, Betrug und rechtlichen Druck Software- und Hardware-Produktentwicklung privater Unternehmen verfälscht hat.

Wir haben gelernt, dass die NSA im Streben nach ihrer bürokratischen Mission, Datenaufklärung in einer zunehmend vernetzten Welt zu leisten, eine systematische Kampagne gegen die Grundwerte US-amerikanischer Macht startete: verfassungsmäßige Gewaltenteilung, technologische Führerschaft und Unternehmertum. Der NSA-Skandal dreht sich nicht mehr nur um Privatsphäre oder einen bestimmten Verstoß gegen verfassungsmäßige oder gesetzliche Auflagen. Die US-amerikanische Politik leidet an einer ernsthaften Autoimmunerkrankung: Unser Abwehrsystem attackiert andere kritische Systeme unseres Körpers.

Als erstes, das Lügen. Die US-amerikanische Geheimdienstuniversität in Washington D.C. bietet einen zertifizierten Studiengang mit dem Namen 'Verläumdung und Hintergehung' als Vertiefung an. Das ist keine absurde Science-Fiction-Dystopie, sondern ein reales Programm, um

Verleumdung und Irreführung durch andere Länder entgegen zu wirken. Die wiederholten Falschdarstellungen lassen vermuten, dass die Geheimdiensteinrichtungen zivile Staatsoberhäupter als Kontrahenten wahrnehmen, mit denen durch Verleumdung und Irreführung umgegangen werden müssen. Vor Monaten haben wir erfahren, dass der Direktor der nationalen Geheimdienste, James Clapper, unter Eid vor dem Kongress gelogen hatte. Wie wir wissen hat jetzt General Keith Alexander eine schriftliche Erklärung abgegeben (vergleichbar mit einer schriftlichen Aussage unter Eid), in der er eine Interpretation von Verstößen von, die laut Gericht ihre »Gutgläubigkeit strapaziere.« Die erst kürzlich veröffentlichte Meinung des Geheimgerichts von 2009 enthält einen ganzen Abschnitt mit dem Titel »Falschdarstellungen vor dem Gericht« und beginnt mit dem Satz:

> *»Dadurch, dass die Regierung dem Geheimdienst-Gericht wiederholt ungenaue Beschreibungen darüber vorgelegt hat, wie ihre Warnlisten gebildet werden, hat sie ihre Nichteinhaltung der Gerichtsbeschlüsse zementiert.«*

General Alexanders Behauptung, dass die hohe Zahl an Verstößen der NSA aufgrund von menschlichem Versagen und Unfähigkeit zustande kamen, erhielt spöttische Aufmerksamkeit. Aber diese Behauptung selbst zielte darauf ab, die Behörde vor Gericht reinzuwaschen, da das ansonsten als absichtlicher Verstoß gegen die Gerichtsbeschlüsse aufgefasst worden wäre. Es gibt absolut keinen Grund, die Behauptungen bzgl. Unfähigkeit und aufrichtigem Fehlverhalten zu glauben – es gibt mehr Gründe anzunehmen, dass diese Behauptungen eine schlimmere Wahrheit verdecken sollen: Absichtliche Verstöße.

Als Zweites, die Staatsgefährdung. Letzte Woche [Anm.: KW37] haben wir gelernt, dass die Strategie der NSA war, allgemeine Sicherheit im Internet zu schwächen, um die eigenen Überwachungsmöglichkeiten zu stärken. Die NSA infiltrierte die sozial-beruflichen Normungsorganisationen, auf denen das gesamte Internet basiert – vom National Institute of Standards and Technology bis hin zur Internet Engineering Task Force, die institutionelle Grundlage des Internets – um die Sicherheitsstandards zu schwächen. Darüber hinaus kombinierte die

NSA Beeinflussung und gesetzlichen Zwang, um kommerzielle Systeme und Standards der meisten grundlegenden Sicherheitssysteme, auf denen das gesamte Internet läuft, zu kompromittieren. Die NSA untergrub die Sicherheit des SSL-Standards, der eine entscheidende Rolle im Online-Banking und Shopping spielt, die von VPN-Produkten, die von zentraler Bedeutung für Unternehmen, Forscher und Gesundheitsdienstleister sind und die von grundlegenden E-Mail-Programmen.

Ernsthafte Leute mit ernsthaften Gesichtsausdrücken warnen, dass Terror und Untergang drohen, wenn wir nicht bedingungslos unsere Geheimdienst-Möglichkeiten ausbauen. Die Aussage ist, dass – was auch immer an kleineren Veränderungen nötig ist – die Einsätze im Kern absolut notwendig sind und Menschen sterben werden, wenn wir zögern. Die Frage bleibt jedoch: Wie viel dessen, was wir haben, ist wirklich notwendig und effektiv und wie viel ist überflüssige Bürokratie, die zu allzu bekanntem Expansionismus und Selbstvergrößerung der Organisation führt?

Die »ernsthaften Menschen« sprechenappelieren an unseren Glauben an die Notwendigkeit nationaler Sicherheit, um verlangen zu können, dass wir eine bestimmte Organisation des Geheimdienstkultes akzeptieren. Die Forderung nach Einhaltung dieses blinden Glaubens ist inakzeptabel.

Was wussten wir tatsächlich darüber, was wir im Austausch dafür erhalten haben, dass die Sicherheit des Internets, Technologiemärkte, das soziale Potenzial des Netzes und die US-amerikanische verfassungsrechtliche Ordnung untergraben wurden? Die Geheimdiensteinrichtungen wuchsen um Milliarden von Dollar, tausende Angestellte und erhielten mehr Macht innerhalb der Exekutive. Und wir, das Volk? Nicht so viel. Gerichtsdokumente, die diese Woche [KW37] veröffentlicht wurden, zeigen, dass das Beste, was die Geheimdiensteinrichtungen den Aufsichtsrichtern nach drei Jahren Arbeit zeigen konnten, war, dass es zu »drei vorläufigen Ermittlungen« kam. Richter Judge Walton bemerkte in seiner Einschätzung, dass dies »nicht sehr signifikant« erscheint.

Falls das das Beste war, was die Geheimdienste im Angesicht richterlicher Sanktionen auf den Tisch legen konnten, können wir annehmen, dass all das Gerede ohne harte, prüfbare und sichtbare Fakten nur darauf abzielte, die Früchte bürokratischer Expansion der letzten Dekade zu schützen. Behauptungen, dass Geheimhaltung die 'Priesterschaft' davon abhielte, solche überprüfbaren Beweise vorzulegen, finden Anklang bei einer Doktrin okkulter Unfehlbarkeit, die wir uns nicht leisten können zu akzeptieren.

Im August haben 205 Mitglieder des Parlaments der Amash-Conyers Gesetzesänderung zugestimmt, die Abschnitt 215 des US PATRIOT Act abgeändert hätte. Der Abschnitt rechtfertigt umfassendes Speichern der Verbindungsdaten inländischer Telefonate. Zu dieser Zeit war dies ein extrem wichtiger Schritt, der sehr genau auf engen und spezifischen Missbrauch abzielte. Aber die Breite und Tiefe organisationeller Irreführung und Staatsgefährdung zwingen uns zu begreifen, dass wir eine Rekonstruktion benötigen, die weitaus tiefer geht als irgendeine spezielle rechtliche Maßnahme.

Wir benötigen eine fundamentale organisationelle Reform. Das sogenannte »betriebsfremde, unabhängige Experten«-Kommitee, das durch den Präsidenten ernannt wurde, mit Insidern der Insider wie Michael Morell und Richard Clarke, wird nicht mal ansatzweise zum gewünschten Ergebnis kommen. Es ist außerdem mehr als unwahrscheinlich, dass dies die Ängste derer mildern wird, die nicht schon Anhänger der Geheimdienstkirche sind.

Unter Beachtung der anhaltenden Lügen und den strategischen Fehleinschätzungen, die durch die Enthüllungen diese Woche [KW37] aufgedeckt wurden, muss die NSA zwangsverwaltet werden. Insider, angefangen bei der Spitze, müssen entfernt und vom Restrukturierungsprozess ausgeschlossen werden. Ihre Expertise hat zu diesem Durcheinander geführt und würde beim Aufräumen nur hindern statt helfen. Wir benötigen einen konsequenten, wahrlich unabhängigen Außenstehenden mit starker und direkter parlamentarischer Unterstützung, der ehemalige, systemkritische Insider, wie Thomas

Drake oder William Binney, rekrutieren würde, um die Leichen im Keller zu finden.

Alles andere als ein radikale Rekonstruktion wäre vergleichbar mit dem Servieren von schwachem Tee für einen Patienten mit einer lähmenden Autoimmunerkrankung.

Dieser Text ist zuerst am 13. September 2013 auf theguardian.com erschienen[166] *und wurde für dieses Buch ins Deutsche übersetzt.*

PRISM: Die EU muss Schritte unternehmen, um Cloud-Daten vor US-Schnüfflern zu schützen

Caspar Bowden

In einer Anhörung im US-amerikanischen Kongress letztes Jahr schüchterte ein Abgeordneter Datenschutz-Befürworter ein, indem er sagte, dass »Fremde in fremden Ländern« überhaupt kein Recht auf Privatsphäre hätten.

Seit den PRISM-Enthüllungen fragt die Welt nicht, was sie mit ihren Daten in US-amerikanischen Cloud-Diensten tun kann, sondern was die USA mit ihren Daten machen können. Im August 2008 hatte der damalige Präsidentschaftskandidat Obama seinen Widerstand gegen ein Gesetz aus der Zeit von Bush aufgegeben, das Abhören ohne richterlichen Beschluss festgeschrieben hat. Wahrscheinlich hatte er sich überlegt, dass er in allen zukünftigen Unstimmigkeiten einen Trumpf in der Hand hätte. FISA Absatz 702 (auch bekannt als FISAAA §1881a) betrifft nicht Amerikaner, es authorisiert den nationalen Geheimdienst (National Security Agency) lediglich, Ausländer außerhalb der USA zu überwachen. Doch durch das – anscheinend unbemerkte – Hinzufügen von lediglich drei Worten forderte das neue Gesetz, dass nicht nur Telekommunikationsunternehmen selbiges befolgen müssen, sondern auch jene Unternehmen, mit deren Diensten man Daten aus der Ferne bearbeiten kann – was wir heute Cloud-Computing nennen.

Die Bedeutung dieser Änderung ist, dass das Abhören von Glasfaser-Kabeln durch Verschlüsselung zwar verhindert werden kann, aber nun können Informationen ganz einfach gesucht und extrahiert werden (in völliger Geheimhaltung) – direkt innerhalb der Lagerhaus-großen Datenzentren, die soziale Netzwerke versorgen und Big Data speisen.

Das Gesetz gilt für jegliche »ausländische Geheimdienst-Informationen«, was folgende Auffang-Definition beinhaltet: »Alles, was ein fremdes Territorium betrifft, das mit der Führung der US amerikanischen Außenpolitik zusammenhängt«, einschließlich politischer Informationen. Es zielt nicht nur

auf mögliche Terroristen und Kriminelle ab, sondern kann auch benutzt werden, um Informationen über das Privatleben, vertrauliche Geschäftsunterlagen und gewöhnliche, rechtsmäßige, demokratische politische Aktivitäten im Rest der Welt zu erlangen.

Die USA beschwichtigen die heimischen Bürger, dass dieses Gesetz nicht auf sie abziele, aber kann es rechtens sein, dass es ein Gesetz für sie und eines für alle anderen gibt? Eine Nachfolge von US-Gerichtsurteilen besagt, dass dies kein verfassungsrechtliches Problem sei. In einer Anhörung im Kongress letztes Jahr schüchtert ein Abgeordneter Datenschutzverfechter ein, indem er sagte, dass »Fremde in fremden Ländern« überhaupt kein Recht auf Privatsphäre hätten.

Beamte der Europäischen Union scheinen zu denken, dass das Verschlüsseln von Daten zur Cloud und zurück von ihr, das Problem beseitige. In ihrem Glauben wurden sie durch verschiedene Berichte aus der Industrie, Anwaltskanzleien, Expertenkommissionen und sogar EU-Behörden bestärkt, da jeder Einzelne zuversichtlich bestätigte, dass das Rechnen in der Cloud sogar sicherer sei. Diese Berichte beachteten jedoch nur die Gefahr durch externe Hacker, nicht das geheime Überwachen durch das hostende Land. Unglücklicherweise gibt es keine praktikablen Abwehrtechniken. Verschlüsselung kann Daten auf dem Transportweg im Kabel schützen, wenn die Daten allerdings durch den Cloud-Anbieter entschlüsselt werden um Berechnungen durchzuführen, sind sie massenhafter Überwachung ausgeliefert.

Zusammen mit Wissenschaftlern erstellte ich 2012 einen Bericht für das Europäische Parlament, der vor der Möglichkeit PRISM-artiger Überwachung warnte, jedoch brauchte es ironischerweise einen US-amerikanischen Blog, um im Januar diesen Jahres Schlagzeilen zu machen. Die europäische Öffentlichkeit reagierte mit verständlicher Beängstigung – vielleicht waren ihre Daten innerhalb der EU gut beschützt, aber was ist mit all den Daten, die durch US-amerikanische Technologie-Giganten verarbeitet werden?

Bestehende europäische Datenschutzgesetze sind nicht nur unzureichend, um Überwachung durch und innerhalb der Cloud zu

entdecken und zu unterbinden, im Kleingedruckten der vorgeschlagenen neuen Datenschutzregulierung, die zur Zeit in Brüssel debattiert wird, werden solche geheimen Veröffentlichungen sogar erlaubt, selbst wenn der Gebrauch unter europäischem Recht rechtswidrig wäre. Wie kamen diese Gesetzeslücken dorthin und warum haben angeblich unabhängige europäische Datenschutzbehörden nichts dagegen unternommen?

Die europäischen Menschenrechte schützen jeden in ihrer Gerichtsbarkeit gleichermaßen und Rechtfertigungen für Verstöße gegen den Datenschutz können nicht auf der Staatsangehörigkeit beruhen. Warum hat die EU-Kommission diese offensichtlichen Konflikte ignoriert und dem Verarbeiten von Daten von EU-Bürgern durch US-amerikanische Cloud-Anbieter grünes Licht gegeben?

Edward Snowden hat nun couragiert die Position verdeutlicht, dass die EU ihm politisches Asyl und Zuflucht gewähren sollte. Es gibt schon Änderungsanträge zur neuen Regulierung, die solche Whistleblower schützen würde. Und auch solche, die besagen, dass die Zustimmung der Bürger notwendig ist, um ihre Daten in der Cloud außerhalb der EU abzulegen – dies außerdem nur nachdem sie einen deutlichen Warnhinweis gesehen haben.

Die USA haben sich der Anerkennung der Europäischen Datenschutzrichtlinien seit 30 Jahren widersetzt und scheinen dies auch weiterhin zu tun. Die EU solle Industrierichtlinien für die eigenen Cloud-Abieter entwerfen, die auf Open Source Software basieren – in einem ähnlichen Ausmaß an Planung, das es nun Airbus erlaubt, die gleichen Marktanteile wie Boeing zu haben. Wenn die Cloud auch nur ansatzweise so wichtig ist wie der Hype suggeriert, warum würde Europa das nicht sowieso tun wollen und die Spitze der Wertkette behalten, die zur Zeit durch steuerliche Vorteile an die USA zurückfließt?

Europa hat eine der besten Forschungen im Bereich Computer-Datenschutz, aber praktisch keine Internet-Unternehmen von globaler Bedeutung. Die Chance für die Märkte ist es, in Jobs und Wachstum

basierend auf Europas Überlegenheit im Datenschutz zu investieren. Die Welt ist gerade im Datenschutz-Guantanamo erwacht, das durch Obama erbaut wurde, aber wir sind keine Gefangenen und uns steht es frei zu gehen.

Dieser Kommentar erschien zuerst am 11. Juli 2013 in der Britischen Zeitung The Independent[167] *und wurde für dieses Buch ins Deutsche übersetzt.*

PRISM, Tempora, Snowden: Analysen und Perspektiven

Thilo Weichert

I. Wir konnten es ahnen

Niemand hätte überrascht sein müssen: Die Mosaiksteine der Bilder der US-amerikanischen und der britischen Telekommunikations- und Internetüberwachung, die mit den Begriffen »PRISM«[168] und »Tempora«[169] bekannt wurden und sich mit den Enthüllungen des US-amerikanischen Whistleblowers Edward Snowden immer weiter präzisierten, sind lange bekannt: Dass die National Security Agency (NSA) für die US-Sicherheitsbehörden weltweit die irgendwie erreichbaren Daten erfassen, weitergeben und analysieren[170] ebenso wie für Großbritannien das Government Communications Headquarters (GCHQ)[171], war in Medien nachzulesen. Die Rechtsgrundlagen für deren Spitzelaktionen, insbesondere der USA PATRIOT Act und der Foreign Intelligence Surveillance Act (FISA) für die USA[172] sowie der Regulation of Investigatory Powers Act (RIPA) für Großbritannien[173], waren bei ihrer Verabschiedung und den späteren Verschärfungen und Verlängerungen jeweils heiß umstritten. Dass NSA und GCHQ riesige Personalapparate und gewaltige Rechenzentren zur Verfügung haben, haben investigative Journalisten auch schon vor längerer Zeit herausgefunden[174]. Das reduzierte Datenschutzverständnis unserer angloamerikanischen und angelsächsischen Freunde westlich und östlich des Atlantiks verursacht uns Datenschützern schon seit Jahren große Bauchschmerzen[175]. Was mit moderner Speichertechnik und Big-Data-Analysen möglich ist, wird uns täglich von der informationstechnischen (IT-) Industrie in Hochglanz angepriesen[176]. Dass tatsächlich gemacht wird, was technisch an Datenspeicherung und -auswertung möglich ist und nützlich erscheint, fürs Geldverdienen

oder für die Sicherheit, wenn niemand Unabhängiges kontrolliert, das wissen zumindest erfahrene Datenschützer seit mehr als drei Jahrzehnten.

Unsere Befürchtung, dass von US-amerikanischen und britischen Sicherheitsdiensten eine gewaltige Gefahr für das ausgeht, was das deutsche Bundesverfassungsgericht im Jahr 1983 »Recht auf informationelle Selbstbestimmung« genannt und begründet hat[177], wird nun durch immer mehr Details zur Gewissheit. Diese Rechtsprechung ist seit 2009 in Art. 8 der Europäischen Grundrechtecharte als »Grundrecht auf Datenschutz« europaweit geltendes Verfassungsrecht und individualrechtlicher Anspruch. Wir müssen dem Edward Snowden unendlich dankbar sein, dass er unsere Unsicherheit beseitigt hat, indem er unsere Befürchtungen bestätigte: Wir wissen seit seinen ersten Enthüllungen, dass die USA und Großbritannien von Hunderten Millionen, ja wohl Milliarden unverdächtigen Menschen sensible Telekommunikations- und Internetdaten auswerten – mit der Begründung, den Terrorismus zu bekämpfen.

II. Nicht Datenschutz contra Sicherheit

Wir wissen, dass die Bekämpfung des Terrorismus oder sonstiger gemeinschädlicher Verbrechen ohne Missachtung unserer Grundrechte möglich ist. Wir wissen, dass eine derartige Grundrechtsmissachtung letztlich in die Hände der Terroristen und Verbrecher spielt: Das deutsche Bundesverfassungsgericht hat entgegen den Empfehlungen von »Sicherheitsexperten« dem deutschen Gesetzgeber immer wieder die rote Karte gezeigt, nachdem dieser den Sicherheitsbehörden weitergehende, manchmal uferlose Befugnisse zuschanzen wollte: großer Lauschangriff, Telekommunikationsüberwachung, KFZ-Kennzeichenerkennung, Rasterfahndung, BKA-Gesetz, Vorratsdatenspeicherung, Antiterrordateigesetz … die Liste der geduldigen, jeweils gut begründeten Urteile und Ermahnungen, im Namen der Sicherheit die Freiheit nicht über Bord zu werfen, ist lang. Für manche mag erstaunlich sein, dass trotz der Einhegung und

Disziplinierung unserer Sicherheitsbehörden die Kriminalität und der Terrorismus in Deutschland erheblich geringer sind als etwa in den USA oder in Großbritannien.

Was für einfache Gemüter erstaunlich sein mag, ist bei nüchterner Betrachtung logisch: Vertrauen ist eine bessere Sicherheitsgrundlage als Angst und Kontrolle. Die Überwachung der gesamten Bevölkerung für Sicherheitszwecke ist unsinnig, weil die meisten Menschen sich im großen Ganzen ehrbar und rechtstreu verhalten. Menschen mit Überwachung zu überziehen, lässt sie an der Ernsthaftigkeit der gesellschaftlichen, politischen und rechtlichen Freiheitsverbürgungen zweifeln und veranlasst sie, dort ihren Vorteil zu suchen, wo die Überwachung nicht ganz so groß erscheint.

Verhältnismäßiges Vorgehen ist insbesondere im Hinblick auf unsere gesellschaftlichen Minderheiten geboten, seien es Muslime, Angehörige arabischer Staaten, Schwule, politisch Andersdenkende oder Menschen mit anderer Hautfarbe oder ungewohntem Aussehen: Als ungerecht empfundene Kontrollen und Überwachung und damit verbundene Ausgrenzung ist der Nährboden für Angst und Aggression bei den Betroffenen. Und dies ist eine wesentliche Grundlage für Hass und Gewaltbereitschaft, bis hin zu terroristischem Fanatismus. Etwas technischer Sachverstand müsste »Sicherheitsexperten« bewusst machen, dass unkontrollierte Kontrollen und insbesondere die Totalkontrolle der Bevölkerung kontraproduktiv sind: Da diese Kontrollen nie völlig perfekt sein können und technische Schutzmaßnahmen eher von den professionellen Kriminellen als den arglosen Bürgern praktiziert werden, geraten außer den Unschuldigen allenfalls kriminelle Amateure bei Rasterfahndungen ins Netz. Den Profis kommen wir nur auf die Schliche, indem wir verdachtsbezogen konkreten Hinweisen gezielt nachgehen[178].

Das vom deutschen Bundesverfassungsgericht geforderte freiheitliche Verständnis von Sicherheit steht in diametralem Widerspruch zum Sicherheitsdenken in Diktaturen oder Überwachungsstaaten wie z.B. China. Es steht aber auch in Widerspruch zur gelebten Sicherheitspolitik

der USA, die sich in ihrer Logik nur wenig von der Russlands oder Chinas unterscheidet. Die US-Realität ist auch möglich, weil es in den USA kein Grundrecht auf Datenschutz, also ein Grundrecht gegen Überwachung, gibt. Von den vom US-Supreme Court eingeforderten »reasonable expectations of privacy« sind bisher Sicherheitsbehörden und Internetfirmen weitgehend ausgenommen[179].

III. US-Kooperation contra Datenschutz

Dies hat Europa ignoriert, als es Kooperationsabkommen mit den USA abschloss, z.B. über die Weitergabe von Fluggast- oder Banktransaktions- oder sonstigen Daten an Sicherheitsbehörden, aber auch mit der Zulassung des transatlantischen Datentransfers zwischen Firmen durch Selbstzertifizierung gemäß den Safe-Harbor-Principles. Dass die »vernünftigen Erwartungen an Privatheit« auch faktisch derart verletzt werden, wissen wir erst seit wenigen Tagen mit Gewissheit. Dadurch ist die Geschäftsgrundlage für die Abkommen zum Datenaustausch weggefallen. Deshalb müssen diese Abkommen hinterfragt und im Zweifel gekündigt werden. Der CDU-Europaparlamentarier Elmar Brok meinte: »Europäer müssen in den USA denselben Rechtsschutz bekommen wie amerikanische Staatsbürger. Diese Forderung ist mit uns nicht verhandelbar«[180]. Die Konferenz der deutschen Datenschutzbeauftragten des Bundes und der Länder wies darauf hin, dass die von der EU-Kommission festgelegten Grundsätze des»sicheren Hafens« (Safe Harbor) zum Datentransfer in die USA (2000) und zu Standardvertragsklauseln zum Datentransfer auch in andere Drittstaaten (2004 und 2010) nur gelten können, wenn bei die Empfänger einem angemessenen Datenschutzniveau unterliegen. Ein Aussetzen der Datenübermittlungen sei möglich, wenn eine »hohe Wahrscheinlichkeit« besteht, dass die Safe-Harbor-Grundsätze oder Standardvertragsklauseln verletzt sind. Dies sei nun der Fall[181]. Damit setzten sie sich von ihrem irischen Kollegen ab, der auch nach Bekanntwerden der NSA-Zugriffe auf Daten von Facebook und Apple keinen Anlass zum Tätigwerden sah und sieht[182].

Neue Abkommen, etwa über eine transatlantische Freihandelszone, sind ohne die Gewährleistung von Datenschutz in den USA angesichts der expandierenden Informationswirtschaft nicht denkbar. Wenn europäische Politiker meinen, sich ökonomisch den Wanst füllen zu können, ohne sich dabei zugleich mit der US-amerikanische Krankheit der Datenschutzverweigerung zu infizieren, betreiben sie Selbst- und Fremdbetrug.

Die Datenschutzignoranz von US-Regierung und US-Industrie verfolgt zwei Ziele: die Erhaltung der globalen sicherheitspolitischen Dominanz und die Bewahrung der Dominanz von US-Informationstechnikunternehmen auf dem Weltmarkt. Diese Ignoranz bzw. dieses Verleugnen wird in den USA leider im Einverständnis von Republikanern und Mehrheitsdemokraten gegen eine aktive Bürgerrechtsopposition durchgesetzt. In dieser Opposition hat Europa mit seinem Grundrechtsverständnis viele natürliche Verbündete. Doch diese Bürgerrechtsopposition hat einen ungemein schwereren Job als die Datenschützer in Europa: Seit über 50 Jahren kämpfen sie für »Privacy and Freedom« – bisher ohne nachhaltigen Erfolg[183].

IV. Edward Snowden

Die Doppelmoral des Vorgangs um PRISM und Tempora zeigt sich am offensichtlichsten am Umgang mit Edward Snowden. Es ist eine Bankrotterklärung der westlichen Gesellschaften, die sich demokratisch und freiheitlich bezeichnen, dass Snowden erst in China und dann in Russland Schutz suchen muss und fand. Es ist erschreckend mit welcher Vehemenz die US-Regierung auf alle Staaten Druck ausübt, die in Frage kommen, Asyl zu gewähren, um eines »Verräters« habhaft zu werden, nicht eines Menschen mit dem Ziel der Verwirklichung von Freiheitsrechte und demokratischer Transparenz. Snowden achtete er sorgsam und bisher erfolgreich darauf, dass durch seine Offenlegung keine Menschen Schaden erleiden. Derweil veranlassen die USA die Zwischenlandung und Durchsuchung des Flugzeugs des bolivianischen Präsidenten Evo Morales in Wien gemäß dem erklärten Motto: »Wir jagen Snowden bis ans Ende der Welt und führen ihn seiner Bestrafung

zu«[184]. Diese Verfolgung ist politische Verfolgung, für die gemäß Art. 16a Abs. 1 GG in Deutschland Schutz gewährt werden muss. Die Bundesregierung ignoriert auch dieses Grundrecht und verweigert die Einreise. Damit begibt sie sich der großen Chance, weitere Informationen zu erlangen, mit denen die USA zu einem Einlenken in Sachen Datenschutz veranlasst werden kann. Während Deutschland die Chance verspielt, mit einer Aufnahme Snowdens, die von ihm erbeten wurde, ein klares Zeichen zu setzen, ist dieser dem politischen Kalkül von Staaten ausgeliefert, deren Gesellschaftsordnung nicht mit seinen – vom europäischen Verfassungsrecht geschützten – Beweggründen und Werten in Einklang stehen[185]. Die freiheitliche Bankrotterklärung erfolgte, als US-Justizminister Eric Holder am 26.07.2013 erklärte, Snowden müsse in den USA keine Todesstrafe und keine Folter befürchten[186].

V. Der Beginn einer langen Auseinandersetzung

Was ist zu tun? Zweifellos müssen die Sachverhalte weiter aufgeklärt werden, und zwar nicht hinter verschlossenen Türen, sondern öffentlich. Hierin kann und darf aber nicht der Schwerpunkt liegen. Das Infragestellen und im Zweifel das Aufkündigen von grundrechtlich nicht akzeptablen Datenaustauschabkommen muss der nächste Schritt sein. Zur rechtlichen Aufarbeitung gehört auch, die straf-, zivil- und vor allem die freiheitsrechtliche Verantwortlichkeit von handelnden Personen und Institutionen zu untersuchen. Sollte die europäische Justiz der »Täter« mit Sitz in den USA nicht so leicht habhaft werden, die britischen Verantwortlichen für die Aktivitäten des GCHQ unterliegen europäischem Recht, das durch die nationalen Regierungen, das Europäische Parlament, den Rat und die Kommission der EU eingefordert werden muss und vor dem Europäischen Gerichtshof in Luxemburg sowie dem Europäischen Menschenrechtsgerichtshof in Straßburg durchgesetzt werden kann.

Die selbstverständlichste Reaktion Europas sollte es sein, die US-amerikanischen Datensauger à la Google, Facebook, Apple, Amazon u. a.

zumindest soweit zur Beachtung des europäischen Rechts zu zwingen, wie diese in Europa aktiv sind. Hierzu können die Verbraucherinnen und Verbraucher einen wichtigen Beitrag leisten. Sie sollten den Unternehmen klar machen, dass sie sich zwischen zwei Alternativen entscheiden können: Die informationelle Ausbeutung und Fremdbestimmung der europäischen Verbraucherinnen und Verbraucher beenden und den Datenschutz zu beachten – oder vom Markt zu verschwinden.

Selbstdatenschutz ist wichtiger denn je. Grundprinzipien sind hierbei Datenvermeidung und Datensparsamkeit, also so wenige Daten im Netz zu hinterlassen wie irgend möglich: Nutzung datensparsamer Internetangebote ohne Datenspuren zu hinterlassen, bei Suchmaschinen z.B. des als datenschutzkonform zertifizierten Ixquick/Startpage. Beim Surfen können Anonymisierungsdienste verwendet werden. Das deutsche Telemediengesetz erlaubt ausdrücklich – entgegen der Praxis von US-Firmen – Pseudonyme statt Klarnamen. Durch Verwendung mehrerer Browser, mehrerer E-Mail-Accounts oder mehrerer sonstiger Identitäten wird eine Profilbildung erschwert. Bei der Datenspeicherung – jedenfalls in der Cloud – und bei sensiblen E-Mails sollten die Daten verschlüsselt werden. Tracking-Blocker und das Löschen von Cookies im Browser erschweren das Tracking. Wenn es bei den Browsereinstellungen schon kein »Privacy by Default« gibt, dann sollte diese gemäß den individuellen Datenschutzwünschen verändert werden.

Bei der Auswahl von Internetdiensten sind europäische und deutsche Angebote den Angeboten aus Drittländern, insbesondere aus den USA, vorzuziehen, weil dann sicher europäisches Datenschutzrecht anwendbar ist. Auch bzgl. britischer Anbieter ist größere Vorsicht und Zurückhaltung geboten. Datenschutzbewusstes Verbraucherverhalten im Internet wird von den Betreibern registriert und eröffnet die Chance, dass sich über den Wettbewerb datenschutzkonforme Produkte durchsetzen[187].

Der Kampf um eine demokratische und freiheitliche Informationsgesellschaft ist noch lange nicht verloren. Dieser Kampf hat

gerade erst begonnen. Bei diesem globalen Kampf stehen uns moderne autoritäre Staaten wie Russland und China gegenüber. Die USA müssen sich entscheiden, auf welcher Seite sie stehen. Wir sollten uns darauf einstellen, eine lange Auseinandersetzung zu führen.

Indien:
Selbst die Regierung vertraut der Regierung nicht

Pranesh Prakash

Teil 1

Es gab Berichte darüber, dass die indische Regierung seit 2009 die Einrichtung eines zentralisierten Überwachungssystems (CMS) vorantreibt[188]. Aber das hat keine große Debatte über Privatsphäre ausgelöst. Selbst Nachrichten über die Inbetriebnahme des CMS im April 2013 haben keine große Aufmerksamkeit erfahren. Nachdem ein Kollege am CIS darüber geschrieben hat und es von Human Rights Watch scharf kritisiert wurde[189], begannen mehr Reporter, es als Problem für die Privatsphäre anzuerkennen. Aber es waren letztlich die Enthüllungen von Edward Snowden, die dazu geführt haben, dass die Menschen, zumindest für einen kurzen Zeitraum, aufgehorcht haben und sich gefragt haben: Wie funktionieren Indiens Geheimdienste? Und haben wir ähnliche Systeme zur Massenüberwachung?

Wenig öffentliche Bekanntmachung

In Indien – dem Heimatland des wohl ältesten Geheimdienstes der Welt, dem Intelligence Bureau – gibt es eine seltsame Mischung von großer Transparenz und sehr wenig Rechenschaftspflicht, was Überwachung und Geheimdienste angeht. Viele hochrangige Beamte geben Reportern bereitwillig anonym Auskunft[190], was zu einer Menge an 'inoffiziellem' Wissen über den Stand der Überwachung in Indien führt. Hingegen gibt es nur sehr wenig, was offiziell berichtet wird und noch weniger davon wird in der nationalen Presse und im Parlament diskutiert. Diese fehlende Verantwortlichkeit wird im gleichen Kontext gesehen wie die Art und Weise, in der die Big-Brother-Akronyme (CMS, NATGRID, TCIS, CCTNS, etc.) sowie der Status der Geheimdienstbehörden in Indien eingeführt wurden: Keine davon wurde jemals durch einen Parlamentsbeschluss mit klaren Regeln und Kompetenzgrenzen

eingerichtet. Es gibt überhaupt keine öffentliche Rechenschaftspflicht oder Überprüfung, außer durch eben denjenigen Flügel der Regierung, der die Institutionen und Projekte zuerst eingerichtet hat.

Zentralisiertes Überwachungssystem

Dieser Mangel an Verantwortlichkeit hat dazu geführt, dass die Regierung seit 2006 an einem zentralisierten Überwachungssystem (CMS) gearbeitet hat, das in das ebenfalls eingeführte Telefon-Abörsystem TCIS integriert wurde. Die Kosten betragen mehr als 8 Milliarden Rupien (mehr als das Vierfache der anfänglichen Schätzung von 1,8 Milliarden Rupien) und noch viel wichtiger: Es kostet unser aller Privatsphäre und unsere persönliche Freiheit. Momentan müssen alle Internet Service Provider und Telefonanbieter (zusammengefasst: Telcos) der Regierung direkten Zugriff auf alle Kommunikation geben, die über ihre Leitungen läuft. Das geschieht jedoch im Moment auf dezentrale Art und Weise, und in den meisten Fällen muss die Regierung die Telcos nach den Metadaten fragen (detaillierte Anrufdaten wie: Wer hat wen wie lange wann angerufen? Welche Webseiten wurden besucht? Wem wurde eine bestimmte IP zugewiesen) oder sie zum Abhören aufforden, damit sie die Daten der Regierung zur Verfügung stellen. Darüber hinaus benutzt die Regierung Instrumente (darunter jene, die von Narus erworben wurden, einer Tochtergesellschaft von Boeing, die aus dem israelischen Geheimdienst entsprungen ist), um Zugriff auf riesige Datenmengen zu bekommen, die zwischen mehreren Städten hin- und hergehen, was die Daten der Unterseekabel, die in Bombay ankommen, mit einschließt. Mit dem CMS wird die Regierung von zentraler Stelle aus Zugriff auf alle Metadaten und Inhalte von Kommunikation erhalten, die indische Telekommunikationsnetze durchlaufen. Das bedeutet, dass die Regierung all deine Anrufe mithören kann, all deine SMS, Emails und Chats lesen kann. Sie kennt all deine Googlesuchen, Webseitenafrufe, Benutzernamen und Passwörter, wenn deine Kommunikation nicht verschlüsselt ist.

Man könnte sich fragen: Warum ist das ein Problem, wo die Regierung doch bereits jetzt dezentralen Zugriff hat? Um diese Frage zu beantworten, muss man zuerst in die Gesetze schauen.

Überwachungsgesetze in Indien

Es gibt keine Gesetze in Indien, die Massenüberwachung erlauben. Die beiden Gesetze, die sich mit Abhörung beschäftigen sind der Indian Telegraph Act, 1885 (unter Absatz 5(2) zusammen mit Regel 419A) und der Information Technology Act (IT Act's Absatz 69 zusammen mit den betreffenden Regeln). Beide erlauben die gezielte Überwachung im genehmigten Einzelfall (in nicht dringlichen Situationen) durch den Innenminister oder den Minister in der Abteilung Informationstechnologie. Der Telegraph Act von 1885 weist an, dass das Abhören von Kommunikation nur im Fall eines Notfalls oder der Bedrohung der öffentlichen Sicherheit zulässig ist. Wenn eine dieser beiden Voraussetzungen erfüllt ist, kann sich die Regierung auf einen der folgenden fünf Gründe berufen: »Die Souveränitat und Integrität Indiens, die Staatssicherheit, freundschaftliche Beziehungen zu anderen Staaten oder die öffentliche Ordnung oder die Verhinderung der Anstiftung zum Begehen einer Straftat«.

2008 hat der Information Technology Act viele der Vorkehrungen zur Abhörung aus dem Telegraph Act kopiert, aber diese beiden Voraussetzungen entfernt. (Oh, welch' Ironie, wenn ein koloniales Gesetz die Privatsphäre besser schützt, als eines, das nach Erreichen der Unabhängigkeit verabschiedet wurde!) Der IT Act setzt daher die Schranke für das Abhören hinab. Da die meiste Kommunikation digital ist, Mobilfunk-Telefonate inbegriffen, ist unklar, in welchen Fällen der Telegraph Act angewandt wird und in welchen der IT Act.

Abgesehen von diesen beiden Bestimmungen, die das Abhören betreffen (ohne Berücksichtigung spezieller Antiterrorgesetze), gibt es viele Gesetze, die gespeicherte Metadaten behandeln, und sie alle haben weitaus niedrigere Anforderungen. Laut der Strafprozessordnung benötigt man keinen Gerichtsbeschluss, es sei denn, der Gegenstand ist eine »Post- oder Telefonbehörde« – in der Regel werden Email-Anbieter und soziale Netzwerke nicht als solche betrachtet.

Unbefugter Zugriff auf Kommunikationsdaten ist nicht per se strafbar. Das ist der Grund dafür, dass der Privatdetektiv, der sich Zugriff auf die

Anrufprotokolle von Arun Jaitley, einem Führer der Bharatiya Janata Partei, verschafft hat, unter Vorwand des Betruges angeklagt wurde und nicht wegen Eindringens in die Privatsphäre. Es gibt zwar eine Bestimmung im Telegraph Act zur Bestrafung unbefugten Abhörens, diese beinhaltet jedoch wesentlich geringere Strafen – bis zu drei Jahren Haft – als diejenige, die einen Bürger trifft, der einer Behörde, die abhören, überwachen oder entschlüsseln will, die Mithilfe verweigert – bis zu sieben Jahre Haft gibt es dann laut Abschnitt 69 des IT Acts. Ja, sieben Jahre Haft.

Um die Lächerlichkeit der harten Sanktionen und sowie die Lächerlichkeit von Abschnitt 69 des IT Act ins rechte Licht zu rücken, betrachte man Folgendes: Ein Geheimdienstbeamter, der nationale Geheimnisse preisgibt, könnte für drei Jahre ins Gefängnis gehen; wenn man ein Dokument nicht aushändigen kann, bei dem man gesetzlich dazu verpflichtet ist, kann man laut indischem Strafgesetzbuch mit bis zu einem Monat Haft belangt werden. Weiterhin könnte ein Bürger, der einer Behörde verweigert, seine Daten zu entschlüsseln, einfach von seinem Recht Gebrauch machen, sich nicht selbst belasten zu müssen.

Aber wie schlecht der IT Act auch sein mag, die Regierung hat gesetzmäßig weitaus Schlimmeres getan. In den Lizenzen, welche die Telekommunikationsbehörde ISPs, Mobilfunkanbietern etc. ausstellt, finden sich Regelungen, die sie zwingen, auch ohne richterlichen Beschluss Zugriff auf alle Kommunikationsdaten und -inhalte zu gewähren. Das wird von den existierenden Abhörgesetzen nicht erlaubt. Die Lizenzen nötigen die Mobilfunkbetreiber auch, Verschlüsselung mit weniger als 40 Bit zu benutzen. (Da GSM Netzwerkverschlüsselung-Systeme wie A5/1, A5/2, und A5/3 feste Schlüssellängen von 64 Bit haben, benutzen die Anbieter scheinbar A5/0, das heißt, überhaupt keine Verschlüsselung. Das bedeutet, dass jeder – nicht nur die Regierung – Techniken zum Abfangen aus der Luft benutzen kann, um Anrufe mitzuhören.)

Laut Regeln, die von der Regierung erlassen wurden, sind Internetcafés – aber nicht Telefonzellen-Betreiber – verpflichtet, detaillierte Daten zu den Indentitätsnachweisen ihrer Kunden, zu deren Fotos und den

Webseiten, die sie besucht haben, für mindestens ein Jahr zu speichern. Gemäß den Regeln, die als Indisches Datenschutzgesetzt (oh, welch' Ironie!) erlassen wurden, müssen den Regierungsbehörden sensible persönliche Daten mitgeteilt werden, wenn sie »für die Verifizierung der Identität oder das Verhindern, Erkennen, Ermitteln, Verfolgen und Berstrafen von Vorfällen, eingeschlossen Cyber-Kriminalität« erforderlich sind.

In den Regelungen, die beschreiben, wann ein Internet-Intermediär für die Aktionen seiner Nutzer verantwortlich ist, gibt es eine Bestimmung mit ähnlicher Begründung, die von Internetfirmen verlangt, dass sie »befugten Regierungsbehörden Informationen und Unterstützung in Sachen investigativer, protektiver Cybersicherheits-Aktivitäten bieten«. (Inkohärente, vage und grammatikalisch falsche Sätze sind ein konsistenter Bestandteil von Gesetzen, die vom Kommunikations- und IT-Ministerium verfasst wurden; eine der Telekommunikationslizenzen besagt: »Der Lizenznehmer sollte Vorkehrungen zum Überwachen gleichzeitiger Anrufe der Sicherheitsbehörden treffen«, wobei sicherlich »zum gleichzeitigen Überwachen von Anrufen duch die Sicherheitsbehörden« gemeint war.)

Der Indische Obergerichtshof hat darauf hingewiesen: »Telefonüberwachung ist ein tiefer Eingriff in die Privatsphäre. Natürlich führt jede Regierung, sei sie noch so demokratisch, bis zu einem gewissen Grad Sub Rosa Operationen als Teil ihres Geheimdienstprogrammes durch, aber gleichzeitig muss das Bürgerrecht auf Privatsphäre vor Missbrauch durch die derzeitigen Authoritäten geschützt werden.« Demnach müssen Regierungen zweifelsohne eine explizite Erlaubnis der Gesetzgebung haben, um ihre elektronischen Überwachungsmöglichkeiten auf welche Art auch immer zu erweitern. Dennoch hat die Regierung sich ohne die Einführung neuer Gesetze wiederholt selbst das Recht zur Abhörung gegeben – ohne, dass das Parlament zugestimmt hat –, indem sie die Berechtigungen in Vertragsbestimmungen und abgeleitete Rechtsvorschriften eingeschleust hat.

Man könnte einwenden, dass die meisten dieser Gesetze den Datenschutzrichtlinien zuwiderlaufen, die in einem Report der Justice A.P. Shah-geführten Gruppe von Datenschutzexperten verkündet wurden, welche der Regierung im Oktober 2012 vorgelegt wurden.

Teil 2

Warum wir der Regierung nicht vertrauen können

Die Reaktion der Regierung auf Kritik an dem CMS könnte sein, dass die bloße Möglichkeit zur Massenüberwachung noch nicht bedeutet, dass sie auch durchgeführt wird. Die Bürokraten werden argumentieren, dass sie sich immer noch an die (schwachen) Gesetze halten werden und sicherstellen, dass jede Überwachungsinstanz befugt ist. Vielmehr werden sie sogar behaupten, dass das CMS Dinge verbessern wird. Es wird die Telcos ausschließen, die Quelle von Datenlecks sein können; es wird sicherstellen, dass jede Abhöranfrage aufgezeichnet wird und der mitgeschnittene Inhalt ordnungsgemäß innerhalb von sechs Monaten gelöscht wird, wie es das Recht verlangt; es wird schnellere Abhörmaßnahmen ermöglichen, die mehr Leben retten werden.

Hier kommen Gründe, warum wir solche Behauptungen zurückweisen sollten:

1. Der Ausschluss der Telcos wird nicht helfen, uns vor Überwachung zu schützen, da die Telcos immer noch die notwendige Infrastruktur zur Durchführung von Überwachung besitzen. Solange die Abhörinfrastruktur existiert, werden Telco-Mitarbeiter sie missbrauchen. In einem gründlichen Bericht aus dem Jahr 2010 bemerkte der Journalist M. A. Arun[191], dass »erschreckenderweise auch diese Korrespondenz durch die Hände mehrerer Angestellter von Serviceprovidern lief, die unberechtigt die persönliche Kommunikation der Kunden abhören.« Als K. K. Paul Sonderpolizeikommissar für Aufklärung war, machte er eine Aktennotiz, in der er die Beschwerden von Mobilfunkanbietern darüber notierte, dass Privatpersonen ihre Kontakte zur Polizei missbrauchten, um Telefongespräche von »Geschäftsrivalen oder zerstrittenen Ehepartnern« abzuhören.

2. Man braucht keine zentralisierten Abhöreinrichtungen, um Abhörnachfragen zentral zu verwalten. Die Dateien sollten zu jeder Zeit mit einer Public-Key Infrastruktur verschlüsselt sein, um unautorisierten Zugriff auf Kommunikationsinhalte, die abgefangen wurden, zu verhindern. Es existieren technische Möglichkeiten, um eine Verarbeitungskette sicher zu überwachen und sicherzustellen, dass das abgefangene Material pünktlich nach sechs Monaten zerstört wird, wie es das Gesetz verlangt. Solche technischen Vorkehrungen und nicht das Zentralisieren der Abhörkapazitäten müssen verpflichtend gemacht werden, um unberechtigten Zugriff zu verhindern.

3. Momentan werden Abhöranordnungen von den zentralen und regionalen Innenministerien ohne angemessene Abwägung erlassen. Nimmt man den Fakt, dass auf zentraler Ebene jeden Monat zwischen 7.000 und 9.000 Telefonüberwachungen autorisiert oder reautorisiert werden, würde es 15 Stunden pro Tag (ohne Einbeziehung von Wochenenden und Feiertagen) dauern, diese 9.000 Anfragen zu bearbeiten, selbst wenn man von nur drei Minuten zur Bewertung jedes Falles ausgeht. Das ließe dem Innenministerium nur wenig Zeit für irgendetwas Anderes. Und wir wissen, dass die Zahlen bei den Bundesstaaten noch viel schlimmer aussehen, jedoch wissen wir nichts Genaueres, da es keine indienweite Statistik über Überwachung gibt.

Das kann nur bedeuten, dass man sich ungenügend damit beschäftigt, oder dass das Verfahren als Regel 419A der Telegraph Rules (das grünes Licht vom Innenministerium für jeden Abhörvorgang erfordert) nicht befolgt wird. Es gibt Gerüchte von Anfragen, die nichts außer einer Telefonnummer beinhalten, gänzlich ohne Erklärung, warum eine Abhörung erforderlich ist. Wir wissen nicht, ob jemals eine Anfrage vom Innenministerium abgelehnt wurde.

4. In einem Verfahren von 1975 hat der Oberste Gerichtshof beschlossen, dass ein »wirtschaftlicher Notfall« nicht einem »öffentlichen Notfall« gleichkommt. Dennoch sehen wir, dass von den neun zentralen Regierungsbehörden, die Presseberichten zufolge das Recht haben, Abhörmaßnahmen durchzuführen – das Central Board of Direct Taxes (CBDT), Intelligence Bureau, Central Bureau of Investigation, Narcotics

Control Bureau, Directorate of Revenue Intelligence, Enforcement Directorate, Research & Analysis Wing, National Investigation Agency und die Defence Intelligence Agency sowie die Staatspolizei – drei sich ausschließlich mit Wirtschaftsdelikten beschäftigen (beziehungsweise vier, wenn man das Central Economic Intelligence Bureau mit einschließt).

Der Verdacht auf Steuerhinterziehung kann keinen Grund zur Telefonüberwachung darstellen. Deshalb rechtfertigte die Regierung das Ausspionieren von Niira Radia, einem Unternehmenslobbyisten, mit der Begründung, er stehe unter dem Verdacht, pakistanischer Spion zu sein. In einem Bericht des Kabinettssekretär von 2011, nach dem Radia-Fall, hat dieser darauf hingewiesen, dass Wirtschaftsverstöße nicht als »öffentliche Notfälle« zählen und dass das Central Board of Direct Taxes keine Berechtigung zur Kommunikationsüberwachung besitzen sollte; seitdem hat sich nichts verändert, denn die Abteilung befindet sich weiterhin auf der Liste derjenigen Behörden, die zur Durchführung von Abhörmannahmen befähigt sein. Das deutet darauf hin, dass man nicht davon ausgehen kann, die Regierung würde sich auch nur im Entferntesten an geltendes Recht halten.

5. Selbst die Regierung vertraut der Regierung nicht. Die Abteilung für Informationstechnologie hat sich kürzlich bei der nationalen Sicherheitsaufsicht darüber beschwert, dass sich die National Technical Research Organisation (NTRO) in die NIC Infrastruktur gehackt habe und auf sensible Daten mehrerer Minsterien zugegriffen habe. Laut der NTRO wurden 2012 hunderte von Email-Konten führender Beamter kompromittiert, einschließlich »dem Innenminister, dem Marineattaché von Tehran, mehreren indischen Delegationen im Ausland, Topermittlern des Central Bureau of Investigation und bewaffneten Streitkräften«. Die indische Armee wurde kürzlich beschuldigt, seine Technical Support Division zu benutzen, um illegal aus der Luft die Telefonanrufe von Politikern in den Bundesstaaten Jammu und Kashmir abzuhören.

Wie können wir davon ausgehen, dass die Regierung die himalayaartigen Informationsmengen schützen wird, die sie mit dem

CMS sammelt, wenn Regierungsbehörden und das Militär andere Regierungsabteilungen und Politiker hacken und ganz offensichtlich nicht einmal der Email-Account des Innenministers sicher ist?

6. Regierungseinheiten nehmen inoffizielle und illegale Überwachung vor, und das CMS wird dem vermutlich kein Ende bereiten.

A. In einem Artikel, der 2010 in Outlook erschien, hat der Journalist Saikat Datta enthüllt, dass verschiedene Bundes- und Landesgeheimdienstbehörden in Indien (illegale) Luft-Abfanggeräte benutzen. »Diese Systeme werden regelmäßig im muslimisch dominierten Stadtgebieten installiert, wie Delhi, Lucknow und Hyderabad. Die Systeme, die in Autos eingebaut sind, werden auf 'Fischfang' geschickt, sie schalten sich zufällig in die Gespräche von Bürgern und versuchen so, Terroristen auzuspüren.

Die National Technical Research Organization (NTRO), die sich nicht einmal in der Liste der abhörberechtigten Institutionen befindet, ist eine der größten Überwachungseinrichtungen Indiens. Der Mint berichtete im letzten Jahr, »NTROs Überwachungsgerät wurden entgegen der Anweisungen öfter in der Nationalhauptstadt installiert als in Grenzregionen« und »gemäß neuer Standardrichtlinien, die früher im Jahr erlassen wurden, darf NTRO nur Signale an den internationalen Grenzen abfangen.«

Die NTRO betreibt mehrere Einrichtungen in Bombay, Bangalore, Delhi, Hyderabad, Lucknow und Kolkata, in denen monumentale Mengen an Internetverkehr abgefangen werden. In Bombay wird aller Verkehr aus den Unterseekabeln abgefangen. Diese schockierende Enthüllung wurde weit vor den Enthüllungen in den Vereinigten Staaten gemacht, dass die NSA die Internet Backbones abschnorchelt, aber sie hat für weitaus weniger Furore gesorgt.

B. Kürzlich wurden in Himachal Pradesh nach einem Regierungswechsel durch die Behörden des Crime Investigation Department (CID) Festplatten beschlagnahmt. Diese enthielten aufgezeichnete Telefongespräche von prominenten Führern der Congress- und Bharatiya Janata Partei, einschließlich dreier früherer Kabinettminister

und naher Verwander mehrerer Ministerpräsidenten, einem Journalisten, vielen hohen Polizeibeamten und dem Generaldirektor der Polizei. Obwohl solche Aufzeichnung laut Gesetz nach sechs Monaten vernichtet werden müssen, wurde das Recht ignoriert und Gespräche bis zurück ins Jahr 2009 wurden gespeichert. Das was uns beunruhigen sollte, ist nicht die Abhörung an sich, sondern die Tatsache, dass ob dieser Telefonabhörung keine Anklage erhoben wurde, was darauf hindeutete, dass sie aus politischen Gründen durchgeführt wurde.

C. In Gujarat enthüllt eine aktuelle Ermittlung des Generaldirektors der Polizei, Amitabh Pathak, dass innerhalb eines Zeitraums von weniger als sechs Monaten mehr als 90.000 Anfragen nach Anrufdetails eingingen, auch für die Telefone führender Beamter von Polizei und öffentlichem Dienst. Diese hohe Zahl lässt sich nicht allein durch die Ermittlung von Straftaten begründen. Und wieder scheint es keinerlei Anklagen gegen irgendeine der Personen gegeben zu haben, deren Daten herausgegeben wurden.

D. Es gibt mehr Überwachungsgeräte, als die Regierung verfolgen kann. Mehr als 73.000 Off-Air-Abhörgeräte wurden seit 2005 nach Indien importiert, und 2011 bat die Bundesregierung verschiedene Landesregierungen, Privatunternehmen, die Armee und Geheimdienstbehörden, diese der Regierung zu überlassen und wies sie darauf hin, dass die Benutzung solcher Geräte illegal sei. Wir wissen nicht, wie viele Geräte tatsächlich eingezogen wurden.

Diese Arten der Verletzung von Privatsphäre kann ernsthafte Konsequenzen nach sich ziehen. Laut dem früheren Geheimdienstchef R.B. Sreekumar aus Gujarat wurden die Anrufprotokolle einer Mobilfunknummer, die von dem früheren Innenminister Gujarats, Haren Pandya, verwendet wurde, zur Bestätigung dafür genutzt, dass er gegenüber dem Concerned Citizens' Tribunal – dem auch ein früherer Richter des Obersten Gerichts angehörte – eine geheime Zeugenaussage gemacht hatte. Dieses Tribunal führte unabhängige Ermittlungen zu der sektiererischen Gewalt 2002 durch, die zum Tod von 2.000 Menschen im Bundesstaat geführt hatte. Haren Pandya wurde 2003 ermordet.

Politisches Händeringen

Wir wissen, dass viele Politiker illegalerweise zum Ziel von Überwachung wurden. Nach dem Indischen Notstand beschrieb die Shah-Kommission, dass der Geheimdienst seine Abhörbefugnisse ungezügelt missbrauchte. Das L. P. Singh Komitee – berufen von der Regierung Janatas – veröffentlichte einen Bericht, der Reformen vorschlug, diese aber wurden niemals umgesetzt. Zahlreiche Politiker von Jagjivan Ram zu HD Deve Gowda und Prakash Karat wurden Gegenstand widerrechtlicher Überwachung. Ramakrishna Hegde trat in den achtziger Jahren des 20. Jahrhunderts sogar zurück, unter Anschuldigung weitreichender illegaler Telefonüberwachung politischer Rivalen, Geschäftsleute und Journalisten.

Dahingegen gab es 2010 großen Aufruhr über die illegale Telefonüberwachung von Bihars Ministerpräsidenten Nitish Kumar, CPM Generalsekretär Prakash Karat und NCP Vorsitzenden Sharad Pawar, der aber zu keinerlei Rücktritten und schließlich auch zu keiner Überholung der Rechenschaftspflichten der Geheimdiensten geführt hat. Der erste Politiker, der eine solche Überholung ansprach, war Vizepräsident Hamid Ansari. Infolgedessen verlangte auch Kongress-Sprecher Manish Tewari öffentlich Reformen und schlug 2001 einen Gesetzesentwurf vor, der eine Rechenschaftspflicht einführen sollte.

Mit diesem Entwurf passierte dasselbe, wie mit allen anderen Gesetzesentwürfen: Nichts. 2012 richtete die Planungskommission eine Expertengruppe unter Justice A. P. Shah ein (Enthüllung: das Centre for Internet and Society war Teil der Gruppe), um existierende Regierungsprojekte zu untersuchen und Grundsätze zu erarbeiten, wie man ein Datenschutzgesetz unter Berücksichtigung internationaler Erfahrungen einführen könnte. Dennoch hat die Regierung den Privacy Act immer noch nicht verabschiedet, der schon so lange in der Schwebe hängt. Als Konsequenz der ständigen Rufe von Datenschutzaktivisten und Anwälten nach einer größeren Rechenschaftspflicht und nach parlamentarischer Aufsicht über die Arbeitsweise und die Ausgaben von Geheimdienstbehörden im Februar 2013 hat das Centre for Public Interest Litigation Klage beim Obersten Gerichtshof eingereicht. Diese würde, so hofft man, zu Reformen führen.

Was Bürger tun sollten

1. Verlangt, dass ein starker Privacy Act inkrafttritt

1991 hat der Leak eines Berichts des Central Bureau of Investigation mit dem Titel »Abhörung der Telefone von Politikern« zu einer Klageschrift der People’s Union of Civil Liberties (PUCL) geführt. Diese hat ausgelöst, dass der Oberste Gerichtshof das Recht auf Privatsphäre in der indischen Verfassung als Bürgerrecht unter Artikel 19(1)(a) (Recht auf freie Rede und Meinungsäußerung) sowie als Menschenrecht unter Artikel 21 (Recht auf Leben und persönliche Freiheit) anerkannt hat, ferner unter den Artikeln 17 der ICCPR und 12 der UDHR.

Trotzdem hat die Regierung durch die Änderungen des Information Technology Act im Jahr 2008, den im Jahr 2011 erlassenen IT Rules und den Telekommunikationslizenzen das Recht auf Privatsphäre, so wie es 1996 im Fall der People’s Union for Civil Liberties vom Obersten Gerichtshof interpretiert wurde, massiv geschwächt.

Wir müssen verlangen, dass dieser Schaden durch starke Datenschutzgesetze rückgängig gemacht wird, die unsere Privatsphäre sowohl gegenüber dem Staat als auch gegenüber Unternehmen schützen. Das Gesetz sollte nicht nur rechtliche Schritte vorsehen, sondern auch sicherstellen, dass Technologien, die diese in Frage stellen, nicht von der Regierung eingesetzt werden dürfen.

Das Gesetz sollte uns auch eine starke Rechtsgrundlage geben, auf der die Massenüberwachung von Indern (über 12.1 Milliarde Datensätze in einem Monat) klar als ungesetzlich benannt werden kann. Das Gesetz sollte sicherstellen, dass das Parlament und die indischen Bürger in regelmäßigen Abständen über die Ausmaße der Überwachung in Indien informiert werden – nicht nur auf zentraler Ebene – und darüber, wie viele Verurteilungen aus dieser Überwachung hervorgingen. Personen, deren Kommunikationsdaten- oder inhalte überwacht oder abgefangen wurden, sollten darüber nach Ablauf einer angemessenen Zeit informiert werden. Und zuletzt sollen Daten nur zur Strafverfolgung von Personen gesammelt werden. Wenn kein Strafantrag gestellt wird,

sollte die Person über das Eindringen in ihre Privatsphäre in Kenntnis gesetzt werden.

Das Gesetz sollte sicherstellen, dass jegliche Überwachung den folgenden Grundsätzen entspricht: Legitimität (Hat die Überwachung eine legitime, demokratische Grundlage?), Notwendigkeit (Ist die Überwachung notwendig, um irgendeinen bestimmten Zweck zu erfüllen? Gibt es weniger invasive Maßnahmen?), Proportionalität und Schadensminimierung (Ist es das minimal mögliche Eingreifen in die Privatsphäre?), Spezifizität (Ist die Überwachungsanordnung begrenzt auf spezifische Daten, Orte oder Personen?), Transparenz (Wird das Eindringen in die Privatsphäre aufgezeichnet und am Ende der betroffenen Person mitgeteilt?), Zweckgebundenheit (Werden die Daten nur für den erklärten Zweck gesammelt?) und unabhängige Aufsicht (Wird über die Überwachung bei einem Gesetzgebungsausschuss oder einem Datenschutzbeauftragten Bericht erstattet? Werden über die durchgeführte Überwachung und die Strafverfolgungsfälle Statistiken erhoben?).

Diese Bestimmungen sollten von einem Verfassungsgericht getroffen werden, also einem Oberlandesgericht oder dem Obersten Gerichtshof. Bürger sollten bei Verstößen gegen die Überwachungsgesetze außerdem das Recht auf Zivilklagen und strafrechtliche Maßnahmen haben. All diese Grundsätze und Praktiken sollten sowohl für Metadaten als auch für Inhalte von Kommunikation gelten, auf Landes- sowie Bundesebene.

Wären das die aktuellen Verfahrensweisen, hätte ein Richter des Obersten Gerichtshofs der Regierung von Gujarat den Zugriff auf diejenigen Metadaten entziehen müssen, die aufgedeckt haben, dass Haren Pandya vor dem Citizen Tribunal ausgesagt hat.

Das Centre for Internet and Society hat einen Gesetzesentwurf ausgearbeitet, der unserer Meinung nach im Sinne der Bürger ist und wir sammeln im Moment Feedback (wir haben bereits alle möglichen Menschen um Rat gefragt – von einem früheren Generalanwalt bis zum Ex-Chef einer Geheimdienstbehörde). Wir hoffen, dass unser Vorschlag zum Vergleich herangezogen werden kann, sobald die Regierung ihren Gesetzesentwurf preisgibt.

2. Wir müssen uns durch Technologie stärken

Anstatt sich auf eine Rechtsreform zu verlassen und Hoffnung in die Regierung zu legen, sollten indische Bürger anfangen, sich mehr um ihre eigene Privatsphäre zu kümmern und ihre Kommunikation zu schützen. Die Lösung ist, Mobiltelefone so selten wie möglich zu benutzen (diese sind Überwachungsgeräte, mit denen man außerdem telefonieren kann, wie es der Gründer der Free Software Foundation Richard Stallman und Andere ausgedrückt haben) und von Anonymisierungstechniken und Ende-zu-Ende-Verschlüsselung Gebrauch zu machen, wenn man über das Internet kommuniziert. Freie und quelloffene Software wie *GnuPG* (eine Implementierung von OpenPGP) können Emails sicher machen.

Auf ähnliche Weise kann man Technologien wie *Off-the-Record Messaging* (OTR) benutzen, das in Anwendungen wie *ChatSecure* und *Pidgin* verwendet wird, um Chatgespräche zu schützen. Außerdem *TextSecure* für SMS, *HTTPS Everywhere* und Virtual Private Networks, um ISPs vom Schnüffeln abzuhalten sowie *Tor* und *I2P*, um den Internetverkehr zu anonymisieren. Es gibt überall in Indien *CryptoParties*, um Menschen beizubringen, wie sie diese und andere freie und quelloffene Software benutzen können, um die Vertraulichkeit ihrer Kommunikation sicherzustellen (speziell jenen, die von Verschlüsselung abhängig sind wie Journalisten, Anwälte, Ärzte etc.).

Auch, wenn jeder seine lokalen Daten verschlüsseln sollte, ist das bei Daten, die ausgetauscht werden, schwieriger. Der Fluch bei Ende-zu-Ende-Verschlüsselung ist, dass beide Enden Verschlüsselung verwenden müssen: Ein Journalist kann kein Off-the-Record Messaging benutzen, wenn seine Quelle es nicht auch benutzt. Solange die Technologie nicht zum Mainstream werden, bleiben sie von denen ungenutzt, die sie wirklich brauchen.

Schlussfolgerung

Die Reaktionen der indischen Regierung auf die Enthüllungen von Snowden sowie die Enthüllungen, dass die Festplatten indischer Botschaften betroffen waren, nahmen die US-Regierung auf

erschreckende Weise in Schutz[192] [193] [194] – ganz im Gegensatz zu dem Standpunkt, den Brasilien klar gemacht hat.

Zwei indische Firmen, die für große Teile der weltweiten Unterseekabel verantwortlich sind, Reliance Communications und die vormals staatseigene Videsh Sanchar Nigam Limited (heute Tata Communications) haben sogar tatsächlich eine Reihe von ‘National Security Agreements’ unterzeichnet, die sie verpflichten, der US-Regierung bei der Überwachung behilflich zu sein[195].

Während wir die Art und Weise beklagen, wie die US-Regierung den Rest der Welt als Untermenschen behandelt, die kein Recht auf Privatsphäre haben, wie es in der Allgemeinen Erklärung der Menschenrechte garantiert wird, müssen wir doch auch sehen, dass die indische Regierung mit Hilfe indischer Unternehmen und unserer Geheimdienste regelmäßig die Privatsphäre indischer Bürger ohne rechtliche Grundlage verletzt. Diese Rechtsverweigerung verschlimmert sich noch durch Projekte wie das CMS, NATGRID etc. Es ist an der Zeit, dass wir uns selbst aufhalten, in schlafwandlerischer Manier auf einen Überwachungsstaat zuzusteuern.

Dieser Text wurde von der Redaktion ins Deutsche übersetzt.

Es ist an der Zeit, die Rechtsstaatlichkeit auf der Welt wiederherzustellen und der Massenüberwachung ein Ende zu bereiten

Katitza Rodriguez

Viele der US-Medienberichte über Edward Snowdens NSA-Enthüllungen haben sich auf deren Einfluss auf die Grundrechte amerikanischer Internetnutzer konzentriert[196]. Das Problem ist aber viel weitreichender als das. Die NSA hat die Kommunikationsdaten von Milliarden Internetnutzern gesammelt und tut es weiterhin. Die persönlichen Informationen von »Nicht-US-Bürgern«, die auf Servern in den USA gespeichert sind oder durch die Netzwerke amerikanischer Firmen laufen, gelten als Freiwild für ungeprüfte Sammlung und Analyse[197]. Dieses unvorstellbare Ausmaß an Überwachung setzt die Rechte jedes Einzelnen gegenüber einer wahllosen und missbrauchten Übermacht des Staates aufs Spiel. Indem das Internet als globaler Spähapparat genutzt wird und jegliche nationalen Datenschutzgesetze über Bord geworfen werden, sind die Grundfesten einer jeden demokratischen Gesellschaft, deren Bürger online kommunizieren, in Gefahr.

Die USA sind nur einer der Übeltäter in der grotesken, unkontrollierten Überwachung[198]. Vor kurzem hat der Kreml seine neueste Überwachungsinfrastruktur in Vorbereitung auf die Olympischen Spiele aufgedeckt[199]. Indiens neues Überwachungssystem bietet zentralisierten Regierungszugriff auf alle Kommunikationsmetadaten und -inhalte, die durch das Telekommunikationsnetz des Landes laufen[200]. Durch die gleichen Leaks, die die Überwachungssysteme der USA ans Licht gebracht haben, wurde auch enthüllt, dass Großbritannien mehr als 200 Glasfaserkabel anzapft, was ihnen Zugriff auf eine riesige Menge an Daten unschuldiger Nutzer gibt[201]. Die

Versuche, die Überwachung in den USA zu reformieren, schneiden ein globales Problem bloß an: Alle Länder ignorieren Menschenrechte, die ihre Spähkapazitäten beeinflussen.

Die Konzepte existierender Menschenrechte haben nicht mit den entstehenden staatlichen Überwachungskapazitäten Schritt gehalten, das schließt die Fähigkeit des Staates ein, einen ganzen Sturzbach an Informationen zu kombinieren und organisieren, um immer detailliertere und feingranular zusammengesetzte Profile von Einzelnen zu erstellen. Entweder fehlt den Regierungen das volle Verständnis der Eingriffstiefe neuer Technologien oder sie nutzen diese Überwachungswerkzeuge wohlweislich aus, um hinter der Fassade der nationalen Sicherheit ihre Kontrollmöglichkeiten zu verstärken.

Um das Problem mit Nachdruck und ganzheitlich anzugehen, haben EFF, Privacy International, Article 19, Access, CIPPIC, Human Rights Watch, CIS India und ein Zusammenschluss von über 275 NGOs versucht, sich auszumalen, wie bestehende Menschenrechtsstandards auf diese neuen, digitalen Überwachungsparadigmen angewendet werden können. Wir haben uns die folgenden Schlüsselfragen gestellt:

- Welche Grundsätze braucht es, um Privatsphäre in der modernen Gesellschaft zu schützen?
- Wie können diese Anforderungen mit den sich ständig entwickelnden Überwachungstechnologien umgehen?
- Was ist unsere Antwort auf das massive, weltweite Aufkommen neuer Überwachungsgesetze und -praktiken?

Als Ergebnis dieser Diskussion haben wir 13 Richtlinien entwickelt, um Staaten auf der ganzen Welt zu erklären, wie existierende Menschenrechte auf Überwachungsgesetze und -praktiken angewendet werden sollten. Die 13 Richtlinien sind in internationalen Menschenrechtsgesetzen begründet und beziehen sich sowohl auf Überwachung innerhalb eines Staates als auch exterritorial. Man findet sie unter necessaryandproportionate.org.

Die 13 Richtlinien verdeutlichen, dass Privatsphäre nur in Ausnahmefällen eingeschränkt werden sollte und das selbst dann jeder Eingriff gesetzmäßig sein muss. Sie sind darauf ausgelegt, politischen Entscheidungsträgern, Richtern, Gesetzgebern, Juristen und der Allgemeinheit Hilfestellung dabei zu geben, über die Begrenzung und Verwaltung solcher Systeme nachzudenken. Die 13 Richtlinien sprechen eine wachsende weltweite Einigkeit darüber an, dass die Überwachung zu weit gegangen ist und zurückgefahren werden muss.

Die Schlüsselelemente der 13 Richtlinien sind im Folgenden skizziert.

Kritische Internet-Infrastruktur schützen

Eine zentrale Richtlinie fordert Staaten dazu auf, die Integrität von Kommunikation und Systemen sicherzustellen. Gesetze, die einer Technologie Sicherheitslücken auferlegen, um Überwachung durchführen zu können, sind grundsätzlich überzogen, sie beeinträchtigen die Privatsphäre und Sicherheit eines Jeden, ganz egal, ob er in irgendein Verbrechen verwickelt ist.

Eine der bedeutendsten Enthüllungen aus dem geleakten NSA-Ausspähprogramm war, wie weit die Behörde gegangen ist, um im Geheimen die sichere Kommunikationsinfrastruktur der Menschen zu unterlaufen[202]. Die NSA ist aggressiv vorgegangen, um die privaten Schlüssel kommerzieller Produkte zu erhalten – das hat es ihnen ermöglicht, unglaubliche Mengen an Internetverkehr zu entschlüsseln, der durch diese Produkte erzeugt wurde. Außerdem haben sie daran gearbeitet, Backdoors in kryptographische Standards einzubauen, die eigentlich die Kommunikation ihrer Nutzer sichern sollten[203].

Datensammlung auf das Nötigste beschränken

Die überstürzte Wandlung hin zu einem Überwachungsstaat gründet sich oft auf dem Glauben, dass Ausspähen ursprünglich auf Terroristen oder Geheimdienstspione abzielte und in jeglicher Rechtsdurchsetzung als Hilfe herangezogen werden sollte. (Ein gutes Beispiel für eine schleichende Ausweitung dieser Ziele ist das Vereinigte Königreich, wo

ein Überwachungsgesetz am Ende einer großen Bandbreite an Regierungsinstitutionen, auch Gemeinderäten und Nahrungsmittelaufsichtsbehörden, Ausspähbefugnisse erteilte.) Die 13 Richtlinien konstatieren, dass Kommunikationsüberwachung[204], einschließlich der Datensammlung, nur in Ausnahmefällen durchgeführt werden kann, wenn gezeigt wurde, dass sie zum Erreichen eines rechtmäßigen und festgeschriebenen Ziels notwendig ist. Kommunikationsüberwachung darf nur durchgeführt werden, wenn andere, weniger invasive Methoden vermutlich fehlschlagen würden.

Metadaten schützen

Es ist nicht mehr akzeptabel, sich auf künstliche technische Unterscheidungen wie 'Inhalt' und 'Nicht-Inhalt' zu verlassen, die als Basis für das massenhafte Zusammentragen persönlicher Daten dienen[205].

Während schon lange Einigkeit darüber herrscht, dass der Inhalt von Kommunikation sensibel ist und wirksamen Schutz durch Gesetze benötigt, ist heute klar, dass andere Informationen, die durch Kommunikation anfallen – beispielsweise Metadaten und andere Arten von Nicht-Inhaltsdaten – möglicherweise sogar noch mehr über einen Einzelnen aussagen als der Inhalt selbst und deshalb die gleichen Schutzmaßnahmen verdienen.

Zum Beispiel gibt es Werkzeuge, die unsere Zugehörigkeiten herausfinden können, indem sie Stückchen vermeintlich nicht-persönlicher Daten benutzen, um uns zu identifizieren und unsere Onlineaktivitäten nachzuverfolgen – so wie: Wer kommuniziert mit wem? Für wie lange? Von wo aus? Die Überwachung von Daten die plausiblerweise Metadaten sind – in etwa der Standort unseres Mobiltelefons, Clickstream-Daten, die erkennen lassen, welche Webseiten man besucht und Search Logs, die anzeigen, nach was man mit einer Suchmaschine wie Google gesucht hat – ist genauso ein Eingriff wie das Lesen von Mails oder das Zuhören bei Telefongesprächen[206].

Was zählt ist nicht, welche Art von Daten gesammelt wird, sondern ihr Effekt auf die Privatsphäre des Überwachungsgegenstandes. Die 13 Richtlinien verlangen, dass eine gut begründete richterliche Anordnung vorliegt, wann immer eine Suche vormals nicht-öffentliche Informationen über die Kommunikation einer Einzelperson hervorbringen wird.

Beenden von Massenüberwachung

Es ist Zeit, Verhältnismäßigkeit wiederherzustellen und dem Kern der Überwachungsgesetze und der Jurisprudenz einen fairen Prozess zu machen. Autoritäten brauchen vorherige Berechtigung durch eine unabhängige und unparteiische richterliche Instanz, die feststellt, dass eine bestimmte Überwachungsmaßnahme mit einer ausreichenden Wahrscheinlichkeit Beweise für ein schwerwiegendes Verbrechen liefern wird.

Jegliche Überwachungsentscheidung muss die Vorteile aus dem Informationsgewinn gegenüber den Kosten der Verletzung von Privatsphäre und freier Meinungsäußerung abwägen. Da der Eingriff durch staatliche, elektronische Überwachung derart massiv ist, sollte Verhältnismäßigkeit erfordern, einen unparteiischen Entscheidungsträger davon zu überzeugen, dass der in Frage stehende Eingriff in die Privatsphäre zu Informationen führen wird, die zur Beseitigung oder Vorbeugung einer ernsthaften Bedrohung beitragen.

Die Rücksicht auf einen fairen Prozess bedeutet auch, dass jeder Eingriff in Grundrechte im Gesetz aufgeführt sein muss und in konsequenter Weise der Öffentlichkeit bekannt gemacht werden muss. Das bedeutet, dass ein Richter sicherstellen muss, dass Grundfreiheiten berücksichtigt werden und Einschränkungen angemessen angewandt werden. Richter müssen immer unparteiisch, unabhängig und kompetent sein, das trifft in besonderer Weise auf Überwachungsmaßnahmen zu. Sie oder er sollte unabhängig von politischer Einflussnahme sein und in der Lage, effektive Kontrolle über den Fall auszuüben.

Bekämpfung einer Kultur der Geheimhaltung

Die Grundlage und Auslegung von Überwachungsbefugnissen müssen öffentlich zugänglich sein und ausnahmslose Aufzeichnungs- und Benachrichtigungspflichten sind notwendig. Das Fehlen von Transparenz in geheimen Regierungsgesetzen und -praktiken zur elektronischen Überwachung spiegeln die fehlende Befolgung von Menschenrechten und geltenden Gesetzen wider.

Geheime Überwachungsgesetze sind nicht hinnehmbar. Der Staat darf keine Überwachungspraktiken übernehmen oder einführen, ohne dass es ein öffentliches Gesetz gibt, dass ihre Grenzen klar absteckt. Darüber hinaus muss das Gesetz ausreichend durchsichtig und präzise sein, sodass der Einzelne über seine Ankündigung Bescheid weiß und seinen Anwendungsbereich einschätzen kann. Wenn Bürger sich eines Gesetzes, seiner Interpretation oder seiner Anwendung nicht bewusst sind, ist es praktisch geheim. Ein geheimes Gesetz ist kein rechtmäßiges Gesetz.

Benachrichtigung muss die Regel sein und nicht die Ausnahme. Einzelne sollten über eine Überwachungsanordnung früh und ausführlich genug informiert werden, damit sie Einspruch gegen die Entscheidung geltend machen können. Sie sollten Zugriff auf die Materialien bekommen, die den Antrag auf die Durchführung der Überwachung unterstützen sollten.

Das Benachrichtigungsprinzip ist wesentlich geworden, um geheime Überwachung zu bekämpfen. Vor dem Internet hat die Polizei an der Tür des Verdächtigen geklopft, die richterliche Anordnung vorgezeigt und dem Betroffenen den Grund für die Hausdurchsuchung genannt. Elektronische Überwachung hingegen ist wesentlich verstohlener. Daten können abgefangen oder direkt von Drittparteien wie Facebook oder Twitter abgerufen werden, ohne dass der Einzelne davon erfährt. Daher ist es oftmals unmöglich zu wissen, dass jemand unter Beobachtung stand, es sei denn die Beweise haben zu einer Anklage geführt. Daher ist es für die Unschuldigen am unwahrscheinlichsten, vom Eindringen in ihre Privatsphäre zu erfahren. Tatsächlich wurden neue Technologien entwickelt, die das Durchsuchen von Heimrechnern aus der Ferne verschleiern.

Die Umstände der Zusammenarbeit von Regierungen und privaten Institutionen müssen öffentlich gemacht werden[207]. Wir kennen die Art des Verhältnisses zwischen Technologieunternehmen oder Internet Service Providern und der NSA nicht. Die 13 Richtlinien verdeutlichen, dass es keinen Spielraum für die freiwillige Zuarbeit von Unternehmen gibt, es sei denn, eine richterliche Anordnung hat den Test auf Verhältnismäßigkeit bestanden.

Schutz des grenzüberschreitenden Zugriffs

Jeder Zugriff auf Daten eines Einzelnen muss in einer Art und Weise stattfinden, die den 13 Richtlinien gerecht wird[208]. Es ist nicht mehr akzeptabel, nationale Datenschutzvorkehrungen zu umgehen, indem man sich auf geheime, informelle Datenaustauschabkommen mit Fremdstaaten oder internationalen Privatunternehmen verlässt[209]. Einzelnen sollten ihre Datenschutzrechte nicht vorenthalten werden, bloß weil sie in einem anderen Land leben[210].

Die übrigen Richtlinien führen Aufsichts- und Schutzmaßnahmen für formelle internationale Zusammenarbeit ein und etablieren Strafen für unrechtmäßigen Zugriff im Allgemeinen. Das beinhaltet Strafen für gesetzwidrigen Zugriff und einen starken und wirksamen Schutz von Whistleblowern. Diese Mechanismen sind wesentlich, wenn man die verborgene Natur elektronischer Überwachungsmaßnahmen betrachtet.

Wir müssen der ungeprüften, anlasslosen, massenhaften Onlineüberwachung ein Ende setzen. Wir müssen die Anwendung von Menschenrechten in die Diskussion über die Kommunikationsüberwachung einbringen. Privatsphäre ist ein Menschenrecht und muss genauso wild entschlossen verteidigt werden wie alle anderen Rechte auch.

Dieser Text wurde von der Redaktion ins Deutsche übersetzt.

Anforderungen an die Ermächtigung zur rechtmäßigen Abhörung

Ian Brown

Ian Brown ergänzt die Debatte über staatliche Internet-Überwachung und die verschiedenen rechtlichen Rahmenbedingungen, die hier Anwendung finden.

Aufgrund von Edward Snowdens Enthüllungen einer umfassenden Internet-Überwachung durch US-amerikanische und britische Regierungen gab es eine große Diskussion über die relativen Vorzüge nationaler rechtlicher Rahmenbedingungen, die notwendige und verhältnismäßige Internet-Überwachung durch Geheimdienst- und Polizeibehörden ermöglichen – einschließlich des SCL-Artikels von Archer, Maxwell und Wolf[211].

Ein wichtiger, aber bisher wenig beachteter Aspekt solcher Rahmenbedingungen ist eine gesetzlich festgelegte Anforderung an Telekommunikationsanbieter, ihre Netzwerke »abhörbar« zu gestalten. Dies erleichtert die Überwachung der Kommunikation – klassischerweise E-Mail oder Ähnliches – aber auch das Abhören jeglicher unverschlüsselter Daten, die durch die Netze reisen, einschließlich der Daten in der Cloud. Dies verringert die Anzahl derer, die über laufende Überwachungen informiert werden müssen, da geschickt platziertes Überwachungs-Equipment Zugriff auf alle Datenströme jeglicher Online-Dienste und Clouds erhält. Dies ermöglicht wesentlich flächendeckendere Überwachung, als dies mit richterlichen oder administrativen Durchsuchungsbefehlen (Mutual Legal Assistance Treaty), die auf einzelne Individuen abzielen, möglich wäre. Da zusätzlich die marginalen Kosten der Überwachung reduziert werden, fördert es die verstärkte Nutzung dieser Methoden. Viele Regierungen haben etwa seit Mitte der 90er Jahre Gesetze verabschiedet, die diese Art der gesetzeskonformen Überwachung ermöglichen sollen – u.a. Folgende:

Land	Gesetz	Jahr

Land	Gesetz	Jahr
Argentinien	Nationales Geheimdienstgesetz Nr. 25.520 Titel VI (National Intelligence Law No. 25.520 Title VI)	2001
Australien	Telecommunications Act §313	1997
Österreich	Überwachungsverordnung	2001
Belgien	Law for the protection of the private sphere against the acts of eavesdropping, gaining knowledge of and opening private communications and telecommunications	1994
Brasilien	Bundesgesetz No. 9.296 (Federal Law No. 9.296)	1996
Estland	Elektronische Kommunikation §§112-114 (Electronic Communications Act §§112-114)	2005
Frankreich	Elektronische Kommunikation §D.98-1 (Posts and Telecommunications Code §D.98-1)	1996
Deutschland	Telekommunikationsgesetz §88 / §110	1996/2004
Indien	Informationstechnologiegesetz, Information Technology Act, Procedure and Safeguards for Interception, Monitoring, and Decryption of Information Rules	2009
Israel	Kommunikationsgesetz (Communications Law)	1982
Malaysia	Kommunikations und Multimediagesetz (Communications and Multimedia Act)	1998
Niederlande	Telekommunikations §13 (Telecommunications Act §13)	1998
Neuseeland	Telekommunikationgesetz (Telecommunications (Interception Capability) Act)	2004
Russland	Kommunikationsgesetz §64 (Law on Communications §64)	2004
Südafrika	Regulierung der Überwachung von Kommunikation und Vorschrift für Kommunikationsrelevante Information (Regulation of Interception of Communications and Provision of Communication-related Information Act Chapter 5))	2002

Land	Gesetz	Jahr
Schweden	Gesetz für elektronische Kommunikation (Electronic Communications Act)	2004
Großbritannien	Telekommunikationsgesetz (Telecommunications Act §94)	1984
	Gesetz zur Regulierung der Geheimdienste (Regulation of Investigatory Powers Act §12)	2000
USA	Communications Assistance to Law Enforcement Act	1994
	FISA Amendments Act §1881a	2008
Kanada	Protecting Children from Internet Predators Act, Bill C–?30	Draft Bill dropped 2013

Die meisten der großen Internetdiensteanbieter haben ihren Sitz in den USA. Daher ist es entscheidend, dass durch den US-amerikanischen Communications Assistance to Law Enforcement Act von 1994[212] (CALEA) alle Telekommunikationsanbieter dazu verpflichtet sind, eine Echtzeit-Überwachung der Kommunikation innerhalb ihrer Netzwerke zu ermöglichen. Außerdem müssen sie detaillierte Anrufprotokolle erstellen. Nach den Anschlägen des 11. Septembers fragten die beiden größten US-amerikanischen Telekommunikationsanbieter (39% und 28% aller internationalen Telefongespräche) die NSA, wie sie ihr helfen könnten. Laut eines zugespielten Berichtes eines NSA Inspector Generals stimmten jene Anbieter und der drittgrößte Anbieter (14% der internationalen Telefonate) zu, in einem »außergewöhnlichen Programm« zu kooperieren, um Metadaten internationaler Kommunikation zu überwachen.

2005 erweiterte die US-amerikanische Federal Communications Commission (FCC) die CALEA Anforderungen auf Breitband-Zugangsanbieter und bestimmte Voice-over-IP-Anbieter. Das Justizministerium fordert außerdem zusätzliche Regulierungen für Zugangsanbieter, um mehr Kommunikationsdaten der Kunden zu speichern. Am 17. Januar 1995 verabschiedeten die Mitgliedsstaaten der

Europäischen Union einen ähnlichen – nicht-bindenden – Ratsbeschluss zur rechtskonformen Telekommunikationsüberwachung[213].

Der britische »Regulation of Investigatory Powers Act 2000« (s 12) ermöglicht es dem Staatssekretär, öffentlichen Telekommunikationsdiensten Verpflichtungen aufzuerlegen, ‘so wie es ihm gerechtfertigt erscheint, um sicherzustellen, dass es durchführbar ist und bleibt, Anforderungen zu erfüllen, um Mithilfe bei der Auferlegung und Durchführung von Überwachungsanforderungen bereitzustellen.’ RIPA 2000, s 8(4) erlaubt es dem Staatssekretär, eine große Bandbreite an richterlichen Anordnungen zu autorisieren, die das Abhören jeglicher Kommunikation, die außerhalb der Britischen Inseln beginnt oder endet, erlaubt. Das scheint die Basis für das britische Tempora Programm zu sein, das vom Government Communications Headquarters (GCHQ) betrieben wird und anscheinend für die Dauer von drei Tagen Mitschnitte eines großen Teils des Internetverkehrs, der britische Grenzen passiert, speichert. Die zugehörigen Kommunikationsdaten werden für 30 Tage aufbewahrt. Die Vereinbarkeit solcher Ausführungen mit der Europäischen Menschenrechtskonvention wurde von drei britischen NGOs – Privacy International, Big Brother Watch und Liberty – vor dem Investigatory Powers Tribunal angefochten.

Parallel dazu haben einige Regierungen Gesetze erlassen – vor allem die EU-Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten –, die Telekommunikationsanbieter dazu verpflichtet, Einträge über die Kommunikation ihrer Kunden zu speichern, jedoch nicht die Inhalte. Diese sogenannten Kommunikations-, Meta- oder Verkehrsdaten beinhalten Details über die gewählte Rufnummer, den Mailabsender und -empfänger sowie die Ortdaten von Mobiltelefonen. Die US Federal Communications Commission verlangt Ähnliches[214]:

> *»Jeder, der Telefondienstleistungen anbietet oder in Rechnung stellt, soll für eine Dauer von 18 Monaten folgende Datensätze aufbewahren, die für die Rechnungsinformationen gebührenpflichtiger Telefonanrufe notwendig sind: Name, Adresse und Telefonnummer des Anrufers,*

Telefonnummer des Angerufenen, Datum, Zeit und Dauer des Gesprächs. Jeder Anbieter muss diese Informationen für gebührenpflichtige Anrufe vorhalten, unabhängig davon, ob er seine eigenen Dienste oder Dienste anderer Anbieter in Rechnung stellt.«

Googles globaler Datenschutzbeauftragter schrieb auf seinem privaten Blog zum Thema 'Wie man Empörung über PRISM vortäuscht':

»Europa hat in Bezug auf die Privatsphäre das invasivste Überwachungsregime der Welt, ausgehend von der verpflichtenden 6- bis 24-monatigen Vorratsdatenspeicherung von Kommunikationsdaten (auch Metadaten genannt), die jede elektronische Kommunikation betrifft. Die USA hat keine solche Vorratsdatenspeicherung, da sie vom US-Kongress als zu tiefer Eingriff in die Privatsphäre abgelehnt wurde. Aber lasst uns nicht darüber sprechen.«

Der Europäische Gerichtshof prüft momentan die Vereinbarkeit der Richtlinie zur Vorratsdatenspeicherung mit der Charta der Menschenrechte, die von nationalen Gerichten in Irland, Deutschland, Bulgarien, Rumänien und der Slowakei in Frage gestellt wurde[215].

Wir wissen auch, dass die US National Security Agency Berechtigungen aus dem USA PATRIOT Act von 2001[216], dem Foreign Intelligence Surveillance Act von 1978 (FISA) sowie dem Amendments Act von 2008[217] (und vor kurzem auch aus einer sehr fragwürdiges Interpretation der 2001 erlassenen Congressional Authorization for the Use of Military Force, die gegen die Angreifer des 11. Septembers gerichtet war) ausnutzt, um Zugriff auf große Mengen an Kommunikationsdaten von US Telekommunikationsanbietern zu erhalten und um das Einrichten von 'Auslandsgeheimdienstmechanismen' in 'Remotediensten' zu erzwingen, die von Firmen wie Microsoft, Google und Apple angeboten werden. Auf diese Weise will die NSA eine großflächige Überwachung des internationalen Datenverkehrs durchführen.

Bei Betrachtung der FCC-Richtlinie (oben zitiert) scheint es, als gäbe es für die US-Regierung keinen Bedarf, Gesetze zur Vorratsdatenspeicherung zu erlassen. Diesen Anschein erwecken auch die Fähigkeiten der NSA, sich selbst Zugang zu einem beträchtlichen Anteil an Kommunikationsdaten zu verschaffen (unter eingeschränkter Aufsicht durch den Foreign Intelligence Surveillance Court, der durch die FISA eingerichtet wurde). Genausowenig sind US-Unternehmen gezwungen, die Datenmenge, die sie über ihre Kunden sammeln, einzuschränken oder die Daten zu löschen, wenn sie nicht mehr für Geschäftszwecke erforderlich sind – beides sind Voraussetzungen für Unternehmen in Vertragsstaaten des Übereinkommens des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[218].

Die USA und die EU-Mitgliedsstaaten haben umfassende verfassungsrechtliche Schutzmaßnahmen, um die Privatsphäre von Einzelnen zu schützen, in denen der Gebrauch von Abhörmaßnahmen durch Regierungsbehörden reguliert wird. Dennoch haben Snowdens Enthüllungen gezeigt, dass die Durchsetzung dieser Regulierungen in Geheimdienstprogrammen schwierig ist. Das gilt aus zwei Gründen besonders in den USA.

Die Bush- und die Obama-Regierung haben vehement ein ‘Staatsgeheimnis’-Privileg durchgesetzt, das die richterliche Kontrolle erschwert. Und der Oberste Gerichtshof wies die mit dem vierten Verfassungs-Zusatzprotokoll begründete Anfechtung des FISA Amendments Acts zurück, die Amnesty International im Namen einiger Anwälte, Journalisten und Menschenrechtsaktivisten eingereicht hatte. Denn die Kläger hätten nicht bewiesen, dass eine Schädigung durch Überwachung »mit Sicherheit bevorstehe«[219]. (Wir werden bald herausfinden, ob die US-Gerichte mehr Willen zum Handeln haben, wenn die konkreten Beweise für die Überwachung, die von Snowden veröffentlicht wurden, vorliegen).

Im Gegensatz dazu hat der Europäische Gerichtshof für Menschenrechte (EGMR) im Fall Klass u.a. gegen Deutschland[220] festgestellt, dass:

»[E]ine Person kann, unter gewissen Voraussetzungen, geltend machen, dass sie durch das bloße Vorhandensein von geheimen Maßnahmen oder von Gesetzgebung, die diese Maßnahmen gestattet, Opfer einer Verletzung sein, ohne behaupten zu müssen, dass solche Maßnahmen tatsächlich gegen sie getroffen worden seien. Die erforderlichen Voraussetzungen müssen für jeden einzelnen Fall bestimmt werden, und zwar entsprechend dem Recht oder den Rechten der Konvention, deren Verletzung gerügt wird, dem geheimen Charakter der angegriffenen Maßnahmen und dem Zusammenhang zwischen dem Betroffenen und diesen Maßnahmen.«

Dies ist einer der Hauptunterschiede zwischen dem geltenden Recht in den Vereinigten Staaten und in Europa, der zu einem besseren Schutz der Privatsphäre bei der Kommunikation im Internet führen dürfte. Ein zweiter Unterschied ist, dass Kommunikationsdaten und andere Auzeichnungen von »Dritten Personen« in den USA nicht unter dem Schutz des 4. Verfassungszusatzes stehen[221], während der EGMR im Fall *Malone v UK* festgestellt hat, dass »die Aufzeichnungen der Telefongebührenzählung Informationen [enthalten], insbesondere die gewählten Nummern, die ein wesentlicher Bestandteil der Kommunikation über Telefon sind. Daraus folgt, dass die Weitergabe dieser Informationen an die Polizei ohne Zustimmung des Teilnehmers auch zu einer Beeinträchtigung mit einem in Artikel 8 garantierten Recht führt.«[222].

Zum Dritten vertritt der Straßburger Gerichtshof die Auffassung, dass nur die Nutzung, nicht aber die Sammlung von Daten einen potentiellen Eingriff in das Recht auf Privatsphäre darstellt, ausdrücklich zurückgewiesen. Leitende US-Regierungsbeamte haben sich bei der Verwendung von Wörtern wie »collection« (engl. »Sammlung«) immer weiter verstrickt, weil sie den Begriff nicht einfach gemäß seiner eigentlichen Bedeutung verstanden haben wollten, sondern als »absichtliche Abfrage oder Auswahl von identifizierten nicht-öffentlichen Kommunikationsvorgängen für die weitere Verarbeitung« (im Original: ‘intentional tasking or selection of identified non-public

communications for subsequent processing'[223]). Im Fall *S. and Marper v UK* dagegen hat der EGMR wiederholt: »Die bloße Speicherung von Daten, die sich auf das Privatleben einer Person beziehen, stellt einen Eingriff i.S.v. Art. 8 EMRK dar.«[224]. Diese Definitionsfragen werden entscheidend sein, *falls* die US-Gerichte sich dafür entscheiden, sich mit den NSA-Überwachugsprogrammen auseinanderzusetzen (etwa durch die Klage des Electronic Privacy Information Center (EPIC) vom 8. Juli 2013 vor dem Obersten Gerichtshof).

Daher kann man sagen, dass die USA zwar nicht als einziges Land von Telekom-Firmen Abfangmöglichkeiten im Netzwerk verlangt, aber die Nutzung dieser Möglichkeiten sich durch verfassungsgegebene Grenzen stark unterscheidet. Wie Judith Rauhofer in ihrer Antwort auf Archer et al. deutlich machte, wird die gerichtliche Durchsetzung dieser Grenzen wohl Zeit benötigen. Aber der Europäische Gerichtshof für Menschenrechte ist bisher nicht davor zurückgeschreckt, sich mit der Geheimdienst-Materie zu beschäftigen. Im Fall *Leander gg. Schweden* kommentierte er, dass 'ein geheimes Überwachungssystem für den Schutz der inneren Sicherheit das Risiko in sich trägt, durch den vorgeblichen Schutz der Demokratie diese zu unterminieren oder gar zu zerstören'[225]. Gut möglich, dass die umfassende Internetüberwachung des Vereinigten Königreichs ebenso wie damals die britische DNA-Datenbank im Fall *S. and Marper* als 'unverhältnismäßiger Eingriff' in die Privatsphäre, der 'in einer demokratischen Gesellschaft nicht als notwendig betrachtet werden kann', bewertet werden würde.

Dieser Artikel ist zuerst am 13. August 2013 bei der Society for Computers and Law *(SCL) erschienen[226] und wurde für dieses Buch ins Deutsche übersetzt.*

Quellen

The Ready Guide to Intercept Legislation 2, SS8 Networks, 2008. Protecting the Public in a Changing Communications Environment, UK Home Office (Cm 7586), 2009, p.8.

The use of the Internet for terrorist purposes, United Nations Office on Drugs and Crime, 2012, pp.47-50. International Data Privacy Law special issue on law enforcement access to private sector data, Oxford University Press, 2012.

How to feign outrage over PRISM, P. Fleischer, 2 August 2013, http://peterfleischer.blogspot.co.uk/2013/08/how-to-feign-outrage-over-prism.html

NSA Office of the Inspector General Review of the President's Surveillance Program, Working Draft ST-09-0002, 2009, http://www.scribd.com/doc/150401523/NSA-inspector-general-report



Wie die Überwachung funktioniert

Die US-Regierung hat das Internet verraten. Wir müssen es uns zurückholen.

Bruce Schneier

Die NSA hat einen fundamentalen Gesellschaftsvertrag verraten. Wir Ingenieure haben das Internet aufgebaut – und nun müssen wir es reparieren.

Die Regierung und die Industrie haben das Internet verraten, und uns.

Indem das Internet auf jeder Ebene untergraben wurde, um es zu einer großen, vielschichtigen und robusten Überwachungsplattform zu machen, hat die NSA einen wesentlichen Gesellschaftsvertrag gebrochen. Die Unternehmen, die die Infrastruktur unseres Internets bauen und pflegen, die Unternehmen, die Hard- und Software herstellen und an uns verkaufen, oder die Unternehmen, die unsere Daten hosten: Wir können ihnen nicht länger vertrauen, dass sie moralische Ordner des Internets sind.

Dies ist weder das Internet, das die Welt braucht, noch das Internet, wie es sich seine Schöpfer vorgestellt haben. Wir müssen es uns zurückholen.

Und mit »uns« meine ich die Gemeinschaft der Ingenieure.

Ja, dies ist vor allem ein politisches Problem, eine Grundsatzangelegenheit, die politische Intervention benötigt.

Jedoch ist es auch ein technisches Problem und es gibt einige Dinge, die Ingenieure unternehmen können – und auch sollten.

Erstens, wir sollten an die Öffentlichkeit treten. Wenn man kein Geheimnisträger ist und falls man keinen National Security Letter mit einem Redeverbot erhalten hat, ist man weder an eine bundesstaatliche Verschwiegenheitspflicht noch an einen Maulkorberlass gebunden. Falls man von der NSA kontaktiert wurde, dass man ein Protokoll oder ein Produkt mit einer Hintertür versehen soll, muss man damit an die

Öffentlichkeit treten. Die Pflichten gegenüber dem Arbeitgeber umfassen kein illegales oder unmoralisches Verhalten. Falls man mit geheimen Daten arbeitet und wahrlich mutig sein will, veröffentlicht man, was man weiß. Wir brauchen Whistleblower.

Wir müssen genau wissen, wie die NSA und andere Behörden Router, Switche, Internet-Backbones, Verschlüsselungstechnologien und Cloud-Dienste untergraben. Ich habe schon fünf Berichte von Menschen wie dir – und ich habe erst mit dem Sammeln angefangen. Ich will 50. Die Masse bringt Sicherheit und diese Art des zivilen Ungehorsams ist eine tugendhafte Tat.

Zweitens, wir können gestalten. Wir müssen herausfinden, wie wir das Internet überarbeiten müssen, um diese Art der massenhaften Überwachung zu verhindern. Wir benötigen neue Techniken, um Vermittler von Kommunikation daran zu hindern, private Informationen preiszugeben.

Wir können Überwachung wieder teuer machen. Vornehmlich benötigen wir offene Protokolle, offene Implementierungen und offene Systeme – diese werden für die NSA schwieriger zu untergraben sein.

Die Internet Engineering Task Force – verantwortlich für die Definition der Standards durch die das Internet funktioniert – hat ein Treffen für Anfang November in Vancouver geplant. Diese Gruppe muss ihr nächstes Treffen dieser Aufgabe widmen. Dies ist ein Notfall und verlangt nach einem Notfalleinsatz.

Drittens, wir können Internet-Regulierung beeinflussen. Bis jetzt habe ich mich dagegen gesträubt, das zu sagen und es macht mich traurig dies nun zu sagen, aber es hat sich gezeigt, dass die USA ein unethischer Verwalter des Internets sind. Großbritannien ist nicht besser. Die Taten der NSA legitimieren den Missbrauch des Internets durch China, Russland, Iran und andere. Wir müssen uns neue Mittel zur Internet-Regulierung überlegen, Mittel die es mächtigen Technologie-Staaten erschweren, alles zu überwachen. Zum Beispiel müssen wir Transparenz, Aufsicht und Rechenschaft von unseren Regierungen und Unternehmen fordern.

Unglücklicherweise spielt dies direkt in die Hände totalitärer Regierungen, die das Internet ihres Landes kontrollieren wollen, um noch extremere Formen der Überwachung zu ermöglichen. Auch hier müssen wir uns überlegen, wie das verhindert werden kann. Wir müssen die Fehler der International Telecommunications Union vermeiden, die zu einem Forum wurde, um schlechtes Regierungsverhalten zu legitimieren. Wir müssen eine wirklich globale Internetregulierung erschaffen, die nicht durch ein einzelnes Land beherrscht oder missbraucht werden kann.

Wenn Menschen aus späteren Generationen auf diese frühen Jahrzehnte des Internets zurückblicken hoffe ich, dass sie nicht von uns enttäuscht sein werden. Wir können dies nur sicherstellen, wenn jeder diese Aufgabe zu einer Priorität macht und an der Debatte teilnimmt. Wir haben eine moralische Pflicht, dies zu tun und wir haben keine Zeit zu verlieren.

Der Abbau des Überwachungsstaates wird nicht einfach sein. Hat irgendein Land, das seine Bürger massenhaft überwacht, freiwillig diese Möglichkeit aufgegeben? Hat irgendein Land, das massenhaft überwacht, es verhindert, totalitär zu werden? Was auch immer geschieht, wir werden neue Wege beschreiten.

Nochmals, die politische Aufgabe ist größer als die technische, jedoch ist die technische Aufgabe entscheidend. Wir müssen verlangen, dass bei diesen Fragen echte Technologen in jede essentielle Entscheidungsfindung der Regierung involviert sind. Wir haben die Nase voll von Anwälten und Politikern, die die Technologie nicht völlig verstehen. Wir brauchen Technologen in der Runde, wenn Technikrichtlinien entworfen werden.

Den Ingenieuren sage ich Folgendes: Wir haben das Internet entworfen und manche von uns haben geholfen, es zu untergraben. Jetzt geht es darum, dass all jene von uns, die die Freiheit lieben, es wieder reparieren.

Dieser Text wurde von der Redaktion ins Deutsche übersetzt.

Wieviel Überwachung ist zu viel?

Richard Stallman

Dank Edward Snowdens Enthüllungen und den wiederholten Verfolgungen und Belästigungen von Journalisten, Informanten und Dissidenten durch die britische und US-amerikanische Regierung wissen wir, dass das derzeitige Ausmaß an Überwachung der Gesellschaft mit den Menschenrechten unvereinbar ist. Es gibt viel zu viel Überwachung. Um unsere Freiheit wiederzuerlangen und Demokratie wiederherzustellen, müssen wir die Überwachung reduzieren. Aber wie weit? Wo genau ist der Punkt, an dem Überwachung zu viel wird?

Angriff auf Journalismus und Meinungsverschiedenheit

2011 erzählte ein unbenanntes Mitglied der US-amerikanischen Regierung, dass Journalisten durch die Regierung nicht vor Gericht geladen würden, da »wir wissen, mit wem ihr redet«[227]. Manchmal wird auf richterliche Anordnung die Anrufliste eines Journalisten eingefordert, um dies herauszufinden[228]. Wenn Whistleblower sich nicht mehr trauen, Verbrechen und Lügen der Regierung aufzudecken, verlieren wir das letzte Stück effektiver Kontrolle über unsere Regierung. Daher ist es zu viel Überwachung, wenn eine Regierung herausfinden kann, wer mit einem Journalisten gesprochen hat. Es ist zu viel als dass Demokratie überleben könnte.

Natürlich sagt der Staat nicht, dass Journalismus angegriffen wird. Als Vorwand bezeichnet die Regierung Whistleblower als Kriminelle – als Spione oder Verräter. Dadurch wird diese Tätigkeit unsicher.

Opposition und Andersdenkende müssen Geheimnisse vor der Regierung, die gewillt ist auch unlautere Mittel einzusetzen, bewahren können. Die ACLU hat gezeigt, dass die US-Regierung systematisch friedliche Gruppen von Systemkritikern infiltrierte, mit dem Vorwand, dass diese vermeintlich Terroristen enthielten[229]. In Großbritannien

haben Polizisten ausgesagt, sich als Aktivisten ausgegeben zu haben, teils wurden sexuelle Beziehungen mit echten Aktivisten eingegangen und mit dem Verschwinden lässt man Liebhaber und Kinder in Ungewissheit zurück[230].

Sind Informationen erst erfasst, werden sie missbraucht

Wenn die Bevölkerung realisiert, dass das Ausmaß allgemeiner Überwachung zu hoch ist, ist die erste Reaktion, Schranken zum Zugriff auf diese akkumulierten Daten einzuführen. Das klingt zunächst schön, jedoch wird es nicht das Problem lösen, nicht einmal ansatzweise, anzunehmen, dass der Verdacht eines Verbrechens einer der Gründe zum Zugriff auf die Daten ist. Ist ein Whistleblower erstmal der »Spionage« beschuldigt, ist das Auffinden des »Spions« ausreichende Begründung, um auf die akkumulierten Daten zuzugreifen.

Kurz gesagt, sind die Daten erstmal erfasst und der Staat hat Zugriff auf selbige, wird es immer möglich sein, diese Daten mit maximalem Schaden zu missbrauchen. Um Journalismus zu schützen, müssen wir die Erfassung von Daten limitieren, auf die der Staat leicht zugreifen kann.

Die Regierungsmitarbeiter, die für die Überwachung zuständig sind, werden diese außerdem für persönliche Zwecke missbrauchen. Einige NSA-Mitarbeiter nutzten das US-Überwachungssystem, um ehemalige, gegenwärtige und potenzielle Liebhaber zu verfolgen – diese Taktik wurde als »LoveInt« (Love Intelligence) betitelt. Die NSA sagt, dass die Verantwortlichen erfasst und bestraft wurden – wir wissen allerdings nicht, wie viele Verantwortliche die NSA nicht aufdecken konnte.

Diese Ereignisse sollten uns nicht überraschen, denn auch die Polizei benutzt oft den Zugang zu Führerschein-Listen, um attraktive Autofahrer zu identifizieren und zu verfolgen – die Strategie ist bekannt als »running a plate for a date« (Ein Kennzeichen für eine Verabredung)[231]. Überwachungsdaten werden immer auch für andere Zwecke benutzt werden, selbst wenn dies verboten ist.

Abhilfe: Daten verstreut lassen

Um trotz Überwachung die Privatsphäre zu schützen gibt es den Weg, die Daten verstreut aufzubewahren und den Zugriff zu erschweren. Klassische Sicherheitskameras waren keine Gefahr für die Privatsphäre. Die Aufzeichnungen wurden meist auf dem Gelände gespeichert und nur für wenige Wochen aufbewahrt. Auf die Daten wurde nur zugegriffen, wenn jemand ein Verbrechen in dem Gebiet meldete. Da der Zugang zu diesen Daten umständlich war, kam es auch nie zu massenhaftem Zugriff. Es wäre wenig praktikabel, jeden Tag Millionen von Videobändern zu sammeln, anzusehen oder Kopien zu erstellen. Und all das nur wegen der unwahrscheinlichen Möglichkeit, dass auf einem der Bänder eine Person zu erkennen ist, die mit einem vermeintlichen Journalisten oder Aktivisten spricht.

Heutzutage sind Sicherheitskameras jedoch zu Überwachungskameras geworden: Sie sind mit dem Internet verbunden, damit sie alle gleichzeitig betrachtet werden können. Die Aufnahmen können in einem Datenzentrum abgespeichert und auf ewig aufbewahrt werden. Das alleine ist schon gefährlich, allerdings wird es schlimmer. Fortschritte in der Gesichtserkennung könnten es bald ermöglichen, Journalisten ständig auf der Straße zu überwachen, um zu erfahren, mit wem sie reden.

Internetfähige Kameras haben typischerweise miserable Sicherheitsvorkehrungen, daher kann jeder sehen, was die Kamera sieht[232]. Um Privatsphäre wiederherzustellen sollten wir internetfähige Kameras dort verbieten, wo sie die Öffentlichkeit überwachen – außer wenn sie mobil durch Personen getragen werden. Jedem muss es freigestellt sein, seine Aufzeichnungen gelegentlich zu veröffentlichen, aber die systematische Akkumulation solcher Daten im Internet muss beschränkt werden.

Abhilfe: Unsere Computer schützen

Die NSA schafft Sicherheitslücken in Software und nutzt diese auch, um unsere eigenen Rechner und Router zu infiltrieren[233]. Wenn es sich

dabei nicht um frei verfügbare und offene Software handelt, haben die Benutzer keine Möglichkeit, diese Lücken zu finden und zu schließen. Microsoft hat so beispielsweise die Sicherheit ihres Windows-Betriebssystems sabotiert, indem sie zunächst die NSA über Sicherheitslücken informierten, bevor die Lücken geschlossen wurden[234]. Wir sehen somit, dass proprietärer Software nicht vertraut werden kann.

Um sich diesem Ausspionieren zu widersetzen, müssen alle Nutzer – gerade auch die Regierungsbehörden – zu freier und offener Software[235] wechseln. Software, die durch die Benutzer kontrolliert wird[236]. Die meiste Software ist nicht offen und frei, sondern proprietär und somit wird sie durch eine Entität kontrolliert – gewöhnlicherweise ein Unternehmen. Die Benutzer können die Software weder analysieren noch ändern. Daher sind sie hilflos, falls das Unternehmen durch die NSA oder jemand anderen kompromittiert wird. Wir müssen auf allen Ebenen proprietäre Software aus dem System reißen und durch freie Software ersetzen. Software, die die Freiheit der Nutzer respektiert.

Bekämpfung der Überwachung durch Unternehmen

Die meisten Daten werden durch die eigenen digitalen Geräte der Benutzer gesammelt. Normalerweise werden diese Daten zuerst durch private Unternehmen gespeichert. In Bezug auf Privatsphäre und Demokratie macht es jedoch keinen Unterschied, ob Daten direkt durch die Regierung oder zunächst durch private Unternehmen gesammelt werden, denn die Daten der Unternehmen stehen systematisch auch dem Staat zur Verfügung. Durch PRISM hat die NSA sich Zugang zu den Datenbanken verschiedenster großer Internet-Unternehmen verschafft[237]. So speichert AT&T seit 1987 die Verbindungsdaten jeglicher Telefonate und stellt diese der US-amerikanischen Drogenfahndung DEA auf Anfrage zur Verfügung[238]. Genau genommen

besitzt die US-Regierung zwar diese Daten nicht, praktisch stehen sie ihr aber zur Verfügung.

Um Journalismus zu schützen, müssen wir deswegen nicht nur die Daten begrenzen, die allgemein durch den Staat erfasst werden, sondern auch all jene Daten, die durch private Unternehmen gesammelt werden. Digitale Systeme müssen überarbeitet werden, sodass sie nicht mehr Daten über ihre Nutzer akkumulieren. Falls Unternehmen digitale Daten unserer Aktivitäten benötigen, sollte es ihnen nicht erlaubt sein, diese länger und in größerem Umfang zu speichern, als für die Transaktion mit uns unbedingt nötig.

Bekämpfung der Überwachung durch Werbung und E-Commerce

Ein Grund für das derzeitige Ausmaß an Überwachung im Internet ist, dass Webseiten sich durch personalisierte Werbung finanzieren, die darauf basiert, dass das Verhalten und die Präferenzen des Nutzers verfolgt und analysiert werden. Dies verwandelt eine schlichte Belästigung – Werbung, die man lernt zu ignorieren – in ein Überwachungssystem, das uns schadet. Ganz gleich ob wir davon wissen oder nicht. Weiterhin verfolgen auch übers Internet getätigte Einkäufe den Benutzer.

Wir alle wissen, dass sogenannte »Datenschutzrichtlinien« normalerweise eher Ausreden dafür sind, unsere Privatsphäre zu missbrauchen statt sie zu schützen. Allgemein sammelt ein Unternehmen zu viele Informationen, wenn es eine »Datenschutzrichtlinie« benötigt.

Beide Probleme könnten wir durch ein System aus anonymen Zahlungen beheben – anonym für den Zahlenden, da es nicht darum geht, dass der Empfänger Steuern umgehen kann. Solche Technologien existieren bereits und es geht nun lediglich darum, geeignete unternehmerische Regelungen zu finden, die nicht durch den Staat verhindert werden.

Eine weitere Gefahr, die von Webseiten ausgeht, die private Daten speichern, ist das Eindringen, Erlangen und der Missbrauch durch ‘Cracker’ – Personen, die Sicherheitsvorkehrungen brechen. Dies

beinhaltet z.B. Kreditkarteninformationen. Ein anonymes Zahlungssystem würde diese Gefahr eliminieren, da man nicht in Gefahr sein kann, wenn die Webseite nichts über einen weiß.

Abhilfe gegen Kommunikationsdossiers

Internet Service Provider und Telekommunikationsunternehmen speichern umfangreiche Daten über die Kontakte ihrer Benutzer, wie z.B. getätigte Telefonate oder besuchte Webseiten. Bei Mobiltelefonen speichern sie außerdem die Bewegungsprofile ihrer Kunden[239]. Diese Dossiers werden für sehr lange Zeit abgespeichert – im Falle von AT&T über 30 Jahre.

Durch solche Dossiers ist unbeobachtete Kommunikation unmöglich. Augenscheinlich darf der Staat keinen Zugriff auf diese Daten haben. Es muss illegal sein, diese Daten zu erheben oder abzuspeichern. Zugangs- und Telekommunikationsanbietern darf es nicht erlaubt sein, diese Informationen – ohne richterliche Anordnung zur Überwachung einer bestimmten Partei – lange vorzuenthalten.

Diese Lösung ist nicht absolut zufriedenstellend, da es die Regierung nicht physisch davon abhält, Informationen direkt abzufangen, wenn sie generiert werden – das ist genau das, was die US-Regierung mit vielen oder allen Telekommunikationsunternehmen macht. Wir müssten uns damit zufrieden geben, dies per Gesetz zu verbieten. Dies wäre jedoch bereits besser als der jetzige Zustand, in dem das entsprechende Gesetz (PATRIOT Act) diese Taktiken nicht explizit verbietet.

Abhilfe gegen Überwachung beim Reisen

Wir müssen die digitale Mautgebühr in anonyme Zahlungen umwandeln – die Technologie hierfür wurde schon vor 25 Jahren entwickelt. Systeme zur Erkennung von Kfz-Kennzeichen sollten per Gesetz nur Kfz-Kennzeichen identifizieren und speichern, die auf einer Liste von gesuchten Fahrzeugen (per richterlicher Anordnung) enthalten sind. Ein weniger sicherer Ansatz wäre es, alle Autos lokal für wenige Tage abzuspeichern und diese Daten nicht über das Internet verfügbar zu machen. Diese Daten dürften nur mittels einer Liste von per

richterlichem Beschluss gesuchten Kfz-Kennzeichen durchsucht werden.

Die »No-Fly« Liste sollte abgeschafft werden, da es eine Bestrafung ohne Anklage ist. Es ist akzeptabel, eine Liste von Personen zu führen, die bei der Personen- und Gepäckkontrolle besonders genau untersucht werden. Weiterhin sollten anonyme Passagiere so behandelt werden, als wären sie auf dieser Liste.

Viele Systeme zur Massenbeförderung benutzen Smartcard- oder RFID-Systeme zur Bezahlung. Diese Systeme sammeln persönliche Daten. Falls man einmal den Fehler macht, nicht mit Bargeld zu zahlen, verknüpfen sie dauerhaft den eigenen Namen mit der verwendeten Karte. Außerdem werden jegliche Reisen, die mit der Karte bezahlt wurden, auch gespeichert. Zusammen ergibt dies eine massive Überwachung. Einer von beiden Aspekten der Datensammlung muss eingestellt werden.

Smart Meter, zu schlau für uns

Wenn wir nicht eine totale Überwachungsgesellschaft wollen, müssen wir Überwachung als eine Art ‘soziale Umweltverschmutzung’ begreifen und somit die Auswirkungen auf die Überwachung jedes neuen digitalen Systems untersuchen. In einem ähnlichen Maße, wie wir die Auswirkungen auf die Umwelt eines physischen Systems untersuchen.

Smart Meter werden zum Beispiel damit angepriesen, dass sie dem Stromversorger jederzeit Daten zum Stromverbrauch jedes Kunden übermitteln. Dies ermöglicht es jederzeit zu bestimmen, ob ein Kunde gerade zuhause ist und teilweise sogar zu bestimmen, was derjenige gerade macht.

Diese Überwachung ist unnötig. Die meisten der Vorteile, die ein Smart Meter mit sich bringt, würden auch erreicht werden, wenn der Stromversorger entsprechende Daten an die Geräte senden würde.

Eines der Features einiger Smart Meter ist es, dem Kunden zu zeigen, wie der eigene Verbrauch im Vergleich zum allgemeinen Kundendurchschnitt liegt. Dies wird durch allgemeine Überwachung

realisiert, könnte aber auch ohne jegliche Überwachung implementiert werden. Für den Stromversorger wäre es einfach, den Durchschnitt je Nachbarschaftsregion zu errechnen, indem der Gesamtverbrauch durch die Anzahl an Kunden geteilt wird – das Ergebnis könnte dann an die Smart Meter gesendet werden. Das Gerät jedes Kunden könnte dann den eigenen Verbrauch über eine bestimmte Zeitperiode mit dem allgemeinen Durchschnitt dieser Periode vergleichen – ganz ohne Überwachung des Kunden.

Die Polizei muss überwacht werden

Individuen mit spezieller, durch den Staat verliehener, Macht – wie beispielsweise die Polizei – verwirken ihr Recht auf Privatsphäre und müssen überwacht werden. Da die Polizei es so häufig macht, hat sie ihren eigenen Jargon für Meineid: »Testilying« (‘testify’ und ‘lying’, in etwa gleichzeitig bezeugen und lügen). Das ist wahrscheinlich der Grund, warum die Polizei es so übel nimmt, wenn sie irgendjemand beim Umgang mit der Bevölkerung fotografiert. Fotografen werden oft attackiert, das Equipment wird zerstört und sie werden aufgrund falscher Anschuldigungen verhaftet. Manchmal berichtet die Polizei auch wahrheitsgemäß, aber wir können nicht beurteilen, wann dies geschieht.

Die Polizei sollte daher dazu verpflichtet sein, Kameras zu tragen und diese Kameras sollten alle Interaktionen der Polizei mit der Bevölkerung aufzeichnen. Eine Stadt in Kalifornien registrierte einen Rückgang an polizeilicher Gewalt um 60%, nachdem diese dazu verpflichtet wurde, jederzeit Videokameras zu tragen.

Kapitalgesellschaften müssen überwacht werden

Kapitalgesellschaften sind keine Personen und haben daher keinerlei Anspruch auf Menschenrechte[240]. Wir können ihnen Privatsphäre gestatten, wenn es keinen Grund gibt, dies nicht zu tun. Selbst Unternehmen, die keine Kapitalgesellschaft sind, haben einen geringeren Anspruch auf Menschenrechte, als nicht-unternehmerisches Leben. Es ist daher legitim, Unternehmen dazu zu verpflichten, Details

über Prozesse zu veröffentlichen, die eine chemische, biologische, nukleare, monetäre, technologische oder politische (z.B. Lobbying) Gefahr für die Gesellschaft darstellen könnten – in einem Ausmaß, das die gesellschaftliche Sicherheit bewahrt. Die Bedrohung durch diese Operationen, wie zum Beispiel BPs Ölleck, Fukushima oder die Finanzkrise 2008, überwiegen die Gefahren des Terrorismus. Falls dadurch unternehmerische Geheimnisse veröffentlicht werden, ist das völlig in Ordnung. (Die Gründungsväter unseres Landes empfanden unternehmerische Geheimnisse als so schädigend, dass sie ein Patentsystem einführten, um davon abzusehen.)

Journalismus muss jedoch vor Überwachung geschützt werden, selbst wenn er Teil eines Unternehmens darstellt. Dies beinhaltet die Arbeit, Notizen, Quellmaterial und die Identität von Informanten. Dies bedeutet jedoch nicht, dass jegliche Aktivitäten eines journalistischen Unternehmens geschützt werden müssten. Ganz im Gegenteil, die Beziehungen zwischen Journalismus und anderen Unternehmen (auch anderen unternehmerischen Aktivitäten) sollten der Öffentlichkeit zugänglich sein, da dies zu Befangenheit bei der Berichterstattung führen könnte.

Fazit

Digitale Technologien führten zu einem enormen Anstieg der Überwachung der Bewegungen, Aktivitäten und Kommunikation der amerikanischen Bürger. Es ist weit mehr als noch in den 1990er Jahren und weit mehr, als die Menschen hinter dem Eisernen Vorhang in den 80ern ausgesetzt waren. Und es wäre selbst mit zusätzlichen gesetzlichen Beschränkungen, inwieweit der Staat die akkumulierten Daten benutzen darf, immer noch wesentlich mehr.

Wenn wir nicht der Meinung sind, dass die USA zuvor unter unzureichender Überwachung gelitten hat und deswegen mehr überwacht werden muss als zu Zeiten der Sowjetunion und Ostdeutschland, müssen wir diesen Anstieg umkehren. Das bedeutet, die Anhäufung enormer Datenmengen über Menschen zu stoppen.

Vorratsdatenspeicherung: Warum Verbindungsdaten noch aussagekräftiger sind als Kommunikations-Inhalte

Andre Meister

Telekommunikations-Verbindungsdaten, wie sie bei der Vorratsdatenspeicherung und von den Geheimdiensten der Welt gesammelt werden, verraten intime Details über unser Leben. Diese auf netzpolitik.org immer wieder betonte Aussage bekräftigt jetzt auch ein Informatik-Professor in einem Gutachten. Die möglichen Rückschlüsse aus Verbindungsdaten sind größer als die der Kommunikationsinhalte – und nehmen noch weiter zu.

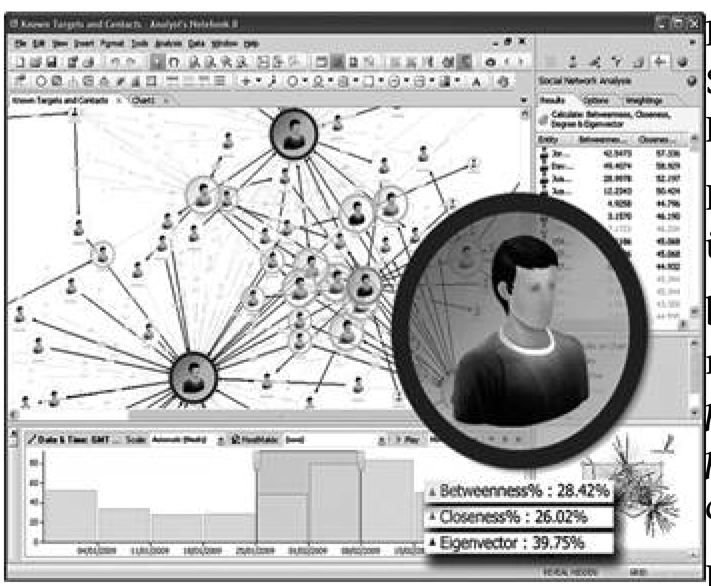
Der Sommer von Snowden begann mit der Enthüllung[242], dass der amerikanische Mobilfunk-Anbieter Verizon alle Telefon-Verbindungsdaten der NSA übermittelt. Das heißt bei uns Vorratsdatenspeicherung. Keine Woche später reichte die American Civil Liberties Union (ACLU) Klage gegen diese krasse Bürgerrechtsverletzung ein.

Der Professor für Informatik und Öffentliche Angelegenheiten Edward W. Felten[243] hat jetzt ein Gutachten an das Gericht übermittelt[244], das zeigt, wie aussagekräftig und intim diese »Metadaten« sind:

> *»Below, I discuss how advances in technology and the proliferation of metadata-producing devices, such as phones, have produced rich metadata trails. Many details of our lives can be gleaned by examining those trails, which often yield information more easily than do the actual content of our communications. Superimposing our metadata trails onto the trails of everyone within our social group and those of everyone within our contacts' social groups, paints a picture that can be startlingly detailed.«*

Metadaten sind einfach zu analysieren

Im Gegensatz zu Inhaltsdaten sind Verbindungsdaten strukturiert: Telefonnummern, E-Mail-Adressen, Zeit und Ort sind einfach zu verarbeiten und miteinander zu verknüpfen. Der kontinuierliche technologische Fortschritt hat die Speicherung günstig und die Rechenleistung möglich gemacht. Dadurch sind neue Möglichkeiten entstanden, große Berge dieser Daten zu rastern und Strukturen zu erkennen.



Dafür gibt es Software von der Stange. Als Beispiel führt Felten i2 Analyst's Notebook[245] von IBM an, über das wir wiederholt berichtet haben[246]. IBM wirbt mit Sprüchen wie: »*Identify key people, events, connections, patterns and trends that might otherwise be missed.*«

Eine weitere in Deutschland eingesetzte Software ist rola rsCASE. Über beide Tools habe ich auch in meinem Talk zur Funkzellenabfrage auf der SIGINT-Konferenz berichtet.

Vor diesem Hintergrund ist es logisch, dass Ermittlungsbehörden und Geheimdienste oft erst Verbindungsdaten analysieren und dann in die Inhalte Verdächtiger hineinzoomen.

Das Produzieren von Metadaten ist unvermeidbar

Im Allgemeinen ist es praktisch unmöglich, in Echtzeit zu kommunizieren, ohne Verbindungsdaten zu hinterlassen. Während Kommunikations-Inhalte verschlüsselt werden können, sind die Metadaten für viele Beteiligte offen. Zwar gibt es Tools wie Tor, um diese zu verschleiern, aber das hilft auch nur zum Teil und hat andere Nebeneffekte.

Telefon-Verbindungsdaten enthüllen Inhalte

Die Verbindungsdaten von Telefongesprächen sind extrem aufschlussreich. Im einfachsten Fall reicht die Zuordnung einer Telefonnummer zu einer Schwangerschafts-, Drogen- oder Spielsucht-Beratung, um von Metadaten auf Inhalte zu schließen. SMS-Nachrichten an bestimmte Nummern können Spenden an Kirchen, eine Familienberatung oder sogar an politische Kandidaten entblößen.

Hierzulande bekannt ist die Visualisierung der Vorratsdaten von Malte Spitz, die extrem viel über sein Leben verrät.

Aggregierte Telefon-Verbindungsdaten sind noch aussagekräftiger

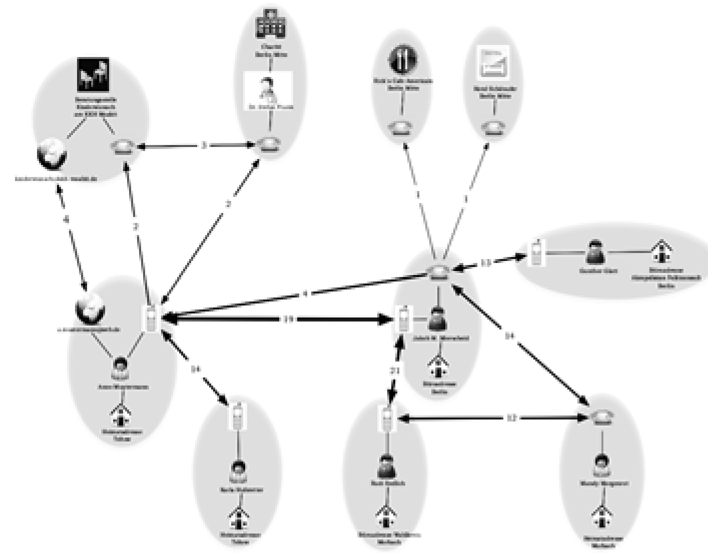
Wenn man Verbindungsdaten sammelt und miteinander verknüpft, werden die daraus gewonnenen Erkenntnisse noch detaillierter. Durch die Erstellung von sozialen Graphen[247] können Rückschlüsse auf soziale Bindungen gewonnen werden. Daran lassen sich sogar[248] der soziale Status und die Hierarchie in einem Unternehmen ablesen. Hier bringt Felten ein aussagekräftiges Beispiel:

> *»A young woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm; followed by a call to a family planning center that also offers abortions. A likely storyline emerges that would not be as evident by examining the record of a single telephone call.«*

Der Chaos Computer Club hat in seinem Gutachten zur Vorratsdatenspeicherung[249] im Juni 2009 bereits ein ähnliches Beispiel visualisiert:

Wer erkennt Muster?

> *»In short, aggregated telephony metadata allows the government to construct social graphs and to study their evolution and communications patterns over days, weeks, months, or even years. Metadata analysis can reveal the rise and fall of intimate relationships, the diagnosis of a life-*



threatening disease, the telltale signs of a corporate merger or acquisition, the identity of a prospective government whistleblower, the social dynamics of a group of associates, or even the name of an anonymous litigant.«

Massenhaft gesammelte Metadaten und Data-Mining über viele Einzelpersonen

Mit den unter dem Buzzword *Big Data*[250] zusammengefassten Entwicklungen der letzten Jahre werden noch erstaunlichere Sachen mit Verbindungsdaten möglich. Einige der Erkenntnisse:

- die Gegenseitigkeit sozialer Beziehungen[251]
- Unterschiede zwischen Festnetz- und Mobilfunk-Nutzer/innen[252]
- das Erstellen detaillierter Gruppenstrukturen[253]
- die Identifizierung von Anrufern anhand ihrer Anruf-Muster unabhängig von Gerät und Nummer[254]
- die Identifizierung des Geräts (ob Fax oder Telefon)[255]
- die Vorhersage, ob ein Gerät dienstlich oder privat genutzt wird[256]
- die Zuordnung des Geräteinhabers zu einer sozialen Gruppe (wie Arbeiter, Pendler oder Student)[257]
- die Vorhersage von Persönlichkeitsmerkmalen einzelner Geräteinhaber[258]

Diese Studien zeigen, dass das Ende der Möglichkeiten noch lange nicht erreicht ist. Es ist auch davon auszugehen, dass die NSA all das kann und macht.

Das Gutachten unterstreicht erneut, wie aussagekräftig die immer als »harmlos« beschriebenen Verbindungsdaten sind. Und dass wir eine anlasslose Speicherung all dieser intimen Details namens Vorratsdatenspeicherung in jeder Form verhindern müssen.

Widerstand gegen Überwachung in nie dagewesenem Ausmaß

Glyn Moody

Obwohl ich als Jounalist bereits seit 20 Jahren über das Internet berichte und als Brite in etwa genauso lange unter Beobachtung der starren Augen von Überwachungskameras gelebt habe, bin ich dennoch überrascht von Edward Snowdens Enthüllungen. Ich hatte schon immer eine sehr zynische Sicht auf Regierungen und ihre Machtinstrumente, wie Polizei und Geheimdienste. Ich habe immer versucht, vom Schlimmsten auszugehen was Überwachung und Angriffe auf meine Privatsphäre anbelangt. Aber ich habe nie geahnt, dass die Regierungen der USA und Großbritanniens mit der Unterstützung anderer Länder zu einer derart totalen und globalen Überwachung fähig wären, wie sie aus den Dokumenten, die Snowden an die Öffentlichkeit gebracht hat, hervorgeht.

Ich glaube, damit stehe ich nicht allein. Manche behaupten nun, dieses Ausmaß der Überwachung sei »offensichtlich« gewesen und der Industrie »wohl bekannt«, aber diesen Eindruck teile ich nicht. Wenn man von den gleichermaßen schockierten und empörten Kommentaren ausgeht, sieht man, dass Bürgerrechtler und Computerexperten – vor allem im Security-Bereich – sich auch niemals vorgestellt hätten, dass die Dinge so schlimm aussehen. Dies führt uns zur naheliegenden Frage: Wie konnte das nur passieren?

In Zusammenhang mit der Empörung aus Kreisen derer, die sich mit solchen Angelegenheiten beschäftigen, gibt es etwas anderes, was der Erklärung bedarf: Das weitestgehende *Ausbleiben* einer Empörung in der normalen Bevölkerung. Natürlich versteht man in manchen Ländern besser als in anderen die Auswirkungen dessen, was Snowden enthüllt hat (manche – vor allem Großbritannien – sind sogar noch schlimmer). Aber angesichts des Ausmaßes und der Kompromisslosigkeit der Ausspähung unserer Onlineaktivitäten fiel die weltweite Resonanz seltsam verhalten aus. Wir müssen verstehen warum, denn sonst wird es

noch schwieriger, zumindest einen Teil dieser Unverhältnismäßigkeiten zurückzufahren.

Die finale Frage, über die dringend nachgedacht werden muss, ist: Was kann man eigentlich tun? Wenn sogar in Ländern wie Deutschland, die normalerweise sehr sensibel auf Angelegenheiten der Privatsphäre reagieren, die öffentliche Resonanz verhältnismäßig gering ausfällt – was sind dann die Alternativen zu einer stärkeren Regierungskontrolle, die in nächster Zeit nicht erwartet werden kann?

Mitte der 90er Jahre bestand eine utopistische Naivität über den Nutzen des Internet. Seit einiger Zeit ist aber klar, dass das Internet auch seine Schattenseiten hat und benutzt werden kann, um Menschen nicht mehr, sondern weniger frei zu machen. Das hat dazu veranlasst, sich von einem komplett offenen Netz weg zu bewegen, in dem alle Informationen unverschlüsselt gesendet werden, hin zu einem, in dem Verbindungen mit HTTPS verschlüsselt werden, um persönliche Informationen vor neugierigen Augen zu schützen. Es ist bemerkenswert, dass der Druck, immer HTTPS zu benutzen, erst in den letzten Jahren angewachsen ist.

Das ist vielleicht auch ein Hinweis darauf, wie die momentane Totalüberwachung zustande kam. Denn obwohl viele wussten, dass unverschlüsselte Daten abgehört werden können, herrschte das generelle Gefühl, es sei nicht möglich, die interessanten Daten herauszufiltern – angesichts der riesigen und immer weiter wachsenden Menge an Daten, die jeden Tag durch digitale Rohre fließen und das Internet darstellen.

Aber es wurde ein entscheidender Faktor übersehen: Moores Law und seine Entsprechungen für Speicherung und Verbindungskapazität. Grob zusammengefasst sagt es, dass die Kosten für Rechenleistung sich in etwa alle 18 Monate halbieren. Umgekehrt heißt das, bei konstanten Ausgaben verdoppelt sich die verfügbare Rechenleistung alle anderthalb Jahre. Und man muss sich in Erinnerung rufen, dass dies ein geometrisches Wachstum darstellt: Moores Law besagt, dass nach 10 Jahren die Rechenleistung sich bei gleichbleibenden Kosten um den Faktor 25 erhöht.

Nun nimmt man noch hinzu, dass die Geheimdienste in ihren Ausgaben für die neueste und schnellste Ausrüstung kaum beschränkt sind, denn es kann immer argumentiert werden, dass die zusätzliche Leistung wesentlich ist, um Informationen zu bekommen, die Leben retten könnten, und so weiter. Eine der ersten und außergewöhnlichsten Enthüllungen Snowdens, die der Guardian an die Öffentlichkeit brachte, gab einen Einblick, wie diese zusätzliche und ständig anwachsende Rechenleistung im sogenannten Tempora-Programm genutzt wird.

Im Sommer 2011 hat GCHQ mehr als 200 Internet-Knotenpunkte angezapft, die jeweils Daten mit der Geschwindigkeit von 10 Gigabit pro Sekunde übertrugen. »Das ist eine massive Menge an Daten!« hieß es in einer internen Präsentation. In diesem Sommer wurden NSA Analysten im Bude-Verfahren vor Gericht gestellt. Im Herbst 2011 startete GCHQ zusammen mit den USA Tempora als Mainstream-Programm

Das Anzapfen der transatlantischen Kabel erschloss GCHQ Zugriff zu speziellen Quellen. Es erlaubte der Regierungsbehörde, Internetpuffer einzurichten, um Daten nicht nur live beobachten zu können, sondern sie auch zu speichern – Inhaltsdaten für drei Tage und Metadaten für 30 Tage.

Das deutet darauf hin, dass Großbritanniens GCHQ Daten mit der Geschwindigkeit von 2 Terrabit pro Sekunde abgriff: heute ist das sicherlich noch viel mehr. Dank Massenspeicherkapazitäten könnte GCHQ den kompletten Internetverkehr von drei Tagen speichern, sowie Metadaten von 30 Tagen.

Es gibt einen einfachen Grund, warum GCHQ so etwas tut: Sie haben gemerkt, dass es nicht nur technisch, bedingt durch Moores Law, sondern auch rechtlich machbar ist. Die britische Rechtsvorschrift, die solche Aktivitäten überwacht – der Regulation of Investigatory Powers Act (RIPA) – wurde 2000 verabschiedet und auf Basis von Erfahrungen der späten 90er Jahre verfasst. Er war dazu bestimmt, das einmalige Abhören von Einzelpersonen zu regeln und behandelt primär die Überwachung von Telefonen und dem Postsystem. Mit anderen Worten wurde er für eine analoge Welt entworfen. Das Ausmaß und die Möglichkeiten *digitaler* Überwachung sind heutzutage derart weit

fortgeschritten, dass der gesetzliche Rahmen von RIPA – trotz seiner Befugnisse – obsolet ist. Im Wesentlichen ist GHCQ also fähig, ohne gesetzliche oder technische Beschränkungen zu operieren.

Der stufenweise, aber unaufhaltsame Wechsel von stückweisem, kleinformatigen Abhören analoger Verbindungen hin zur Totalüberwachung könnte auch helfen, die Gleichgültigkeit der Öffentlichkeit gegenüber den Enthüllungen zu verstehen. Auch über die oberflächliche Idee hinaus, dass derjenige, der nichts zu verbergen hat, auch nichts befürchten muss – jeder hat etwas zu verbergen und seien es bloß die privaten Momente in seinem Leben – gibt es eine andere gebräuchliche Erklärung, warum die Menschen nicht besonders besorgt über die Aktivitäten von NSA und GCHQ sind. Nämlich, dass »niemand sich dafür interessiert«, was sie tun. Daher sind sie zuversichtlich, dass sie durch das Speichern und Analysieren von Internetdaten nichts zu befürchten haben.

Das ist auch in einer grundlegend analogen Sicht auf die Dinge begründet. Natürlich haben diese Menschen Recht, dass kein Spion an einer Tastatur sitzt und ihre E-Mails oder Facebook-Nachrichten liest. Das ist natürlich nicht möglich, selbst wenn es gewollt wäre. Aber das ist auch gar nicht notwendig, denn Daten können von ermüdungsfreien Programmen »gelesen« werden, die dank Moores Law zentrale Informationen mit wachsender Geschwindigkeit und schwindenden Kosten extrahieren.

Die Menschen sind demgegenüber sorglos, denn die meisten können sich gar nicht vorstellen, was die heutigen Supercomputer mit ihren Daten tun können, und denken wieder in analogen Bildern – ein Spion der sich langsam durch einen riesigen Sumpf voller Informationen kämpft. Und das ist auch verständlich, denn selbst Computerexperten haben Schwierigkeiten, mit der Geschwindigkeit der Entwicklungen mitzuhalten und die Auswirkungen abzuschätzen.

Ein Post auf dem Blog von Google Search aus dem letzten Jahr kann helfen, einen Eindruck zu bekommen, wie mächtig heutige Systeme sind:

> *»Wenn Du eine einzige Anfrage in die Google-Suchmaske eingibst oder sie bloß in Dein Telefon sprichst, setzt Du so viel Rechenleistung in Gang wie es brauchte, um Neil Armstrong und elf andere Astronauten zum Mond zu schicken. Nicht nur für den eigentlichen Flug, sondern auch für all die Berechnungen während der Planung und Durchführung des elfjährigen Apollo-Programms mit 17 Missionen.«*

Fügt man jetzt hinzu, dass täglich drei Milliarden Suchanfragen an Google verschickt werden und dass die Rechenkapazität der NSA wahrscheinlich noch wesentlich größer ist als die von Google, bekommt man einen Eindruck der geballten Leistung, die für die Analyse der »trivialen« Daten verfügbar ist, die über uns alle gesammelt werden und wie das zu sehr nicht-trivialen Rückschlüssen über intimste Teile unseres Lebens verhelfen kann.

In Bezug darauf, wie viel Information gespeichert werden kann, schätzt William Binney, früherer technischer Direktor der NSA, dass ein Datencenter, das im Moment in Utah gebaut wird, in der Lage sein wird, fünf Zettabyte Daten verarbeiten und speichern zu können. Wenn man das auf Papier ausdrucken und in klassischen Aktenschränken aufbewahren würde, bräuchte man etwa 42 Millionen Millionen Schränke, die 17 Millionen Quadratkilometer Grundfläche einnehmen würden.

Weder Rechenleistung noch die umfassende Speicherung persönlicher Daten allein bedrohen unsere Privatsphäre und Freiheit direkt. Doch wenn man sie zusammenbringt, kann die NSA nicht nur mehr oder weniger unmittelbar alle möglichen Informationen in 42 Millionen virtuellen Aktenschränken finden, sondern auch alle Wörter und alle Seiten in allen Schränken miteinander in Verbindung bringen – das kann man sich für einen Menschen nicht einmal ansatzweise vorstellen.

Es ist diese beispiellose Fähigkeit, all diese Daten über uns zusammenzutragen und mit den Daten unserer Familie, Freunden und Bekannten, und deren Familie, Freunden und Bekannten (und manchmal sogar deren Bekannten der Bekannten unserer Bekannten) zu kombinieren, die das Ausmaß des Wissens ausmacht, das die NSA

jederzeit zur Verfügung hat. Für die meisten von uns ist es unwahrscheinlich, dass dieses Wissen jemals abgerufen wird. Aber es bedarf bloß einer winzigen Auffälligkeit irgendwo tief in der Kette unserer Bekanntschaften, um eine Verbindung herzustellen und all unsere unschuldigen Datensätze zu beflecken. Das führt dazu, dass sie auf einem riesigen Stapel an Daten landen, der in einer unvorstellbar tiefgreifenden Art und Weise querverwiesen, durchsucht und auf der Suche nach typischen Mustern analysiert wird.

Wenn man dieses nachvollziehbare, aber bedauerliche Unverständnis eines Teils der Öffentlichkeit betrachtet, was die außergewöhnlichen Fähigkeiten der NSA angeht und das, was diese an Ergebnissen extrahieren kann, kommt man zu einer Schlüsselfrage: Was können wir tun, um unsere Privatsphäre zu stärken? Bis vor wenigen Wochen hätten die meisten, die auf diesem Gebiet arbeiten, gesagt: »Alles verschlüsseln.« Aber die aktuellen Enthüllungen darüber, dass NSA und GCHQ es geschafft haben, praktisch jedes weit verbreitete Verschlüsselungssystem zu unterlaufen, scheint auch diese letzte Hoffnung zu zerstören.

Oder vielleicht auch nicht. Es herrscht annähernd Einigkeit unter den Kryptographie-Experten, dass das theoretische Fundament der Verschlüsselung – seine mathematischen Grundlagen – unberührt bleibt. Das Problem liegt in der Implementierung und in dem Zusammenhang, in dem Kryptographie eingesetzt wird. Edward Snowden weiß wahrscheinlich besser als die meisten anderen, wie die Situation wirklich aussieht. Er hat es so ausgedrückt:

> *»Verschlüsselung funktioniert. Richtig umgesetzt sind starke Kryptosysteme eines der wenigen Dinge, auf die man sich verlassen kann. Leider ist Endpoint-Security so furchtbar schwach, dass die NSA ständig Wege findet, sie zu umgehen.«*

Das ist ein extrem wichtiger Hinweis, was wir tun müssen. Es sagt uns, dass an Kryptographie an sich nichts falsch ist, nur an den korrumpierten Implementierungen von sonst starken Verschlüsselungstechniken. Das wurde durch kürzliche Leaks bestätigt,

die zeigen, dass Softwarefirmen daran mitarbeiten, die angeblich sichere Software, die sie verkaufen, zu schwächen – das ist ein grundlegender Betrug des Vertrauen, das Kunden ihnen entgegenbringen.

Die guten Neuigkeiten sind, dass wir eine Alternative haben. In den letzten Jahrzehnten ist mit freier Software und offenem Quelltext ein ganzes Software-Ökosystem entstanden, das sich der Kontrolle traditioneller Computerindustrie entzieht. Das macht eine Unterwanderung durch die NSA wesentlich schwieriger, da der Quellcode offen entwickelt wird. Das ermöglicht es jedem, den Code durchzusehen und nach Backdoors zu suchen – geheime Wege, um zu spionieren und Software zu kontrollieren.

Das heißt nicht, dass freie Software komplett immun gegenüber Sicherheitsproblemen ist. Viele Open Source Produkte stammen von Firmen und es ist vorstellbar, dass auf manche Druck ausgeübt wurde, ihre Teile ihrer Arbeit zu schwächen. Freie Software kann unterwandert werden, wenn sie von dem Quellcode, der sich leicht auf Backdoors überprüfen lässt, in Binärprogramme übersetzt werden, die dann tatsächlich auf dem Computer ausgeführt werden und für die das nicht mehr möglich ist. Es gibt auch die Möglichkeit, in Downloadverzeichnisse von quelloffener Software einzubrechen und diese auf subtile Art und Weise durch gefälschte zu ersetzen.

Trotz dieser Probleme ist Open Source immer noch die größte Hoffnung, die wir haben, wenn es um starke Verschlüsselung geht. Aber in Folge der Snowden-Enthüllungen muss die Free Software Community zusätzliche Vorsicht walten lassen, um das Risiko zu minimieren, dass Code anfällig gegenüber Angriffen und Subversion durch Spionageeinrichtungen ist.

Über solche Maßnahmen hinaus sollte die Open Source Welt auch anfangen, eine neue Generation von Anwendungen zu schreiben, die starke Kryptographie beinhalten. Solche existieren schon, aber sie sind oftmals schwer zu bedienen. Es bleibt mehr zu tun, um sie für einen durchschnittlichen Nutzer brauchbar zu machen: Er mag sich zwar nicht

für die Möglichkeit interessieren, dass NSA und GCHQ seine Onlineaktivitäten überwachen, aber wenn es ein Angebot an guten Werkzeugen gibt, die es einfach machen, solchen Bemühungen vorzubeugen, könnte es sein, dass viele Menschen sie benutzen. Genauso wie viele zum Firefox-Browser gewechselt sind – nicht weil er offene Standards unterstützt, sondern weil er besser ist.

Es gibt keinen Grund, hoffnungslos zu sein, auch wenn das Ausmaß der Spionage, das Snowden enthüllt hat, einem den Atem verschlägt und die Leaks über die tiefgreifende und absichtliche Zerstörung der kompletten Vertrauens- und Sicherheitssysteme des Internets schockierend sind. Selbst angesichts der weitgehenden Ignoranz in der Öffentlichkeit und der Gleichgültigkeit gegenüber der Gefahr, die Totalüberwachung für die Demokratie darstellt, können wir, soweit wir wissen, immer noch starke Verschlüsselung in quelloffener Software benutzen, um unsere Privatsphäre zu schützen.

Das könnte in der Tat eine Möglichkeit für Open Source sein, von einem größeren Publikum angenommen zu werden. Denn wir wissen nun, dass kommerzieller Software nicht mehr vertraut werden kann und sie effektiv Spyware ist, für die man bezahlen muss. Und so wie Moores Law der NSA und GCHQ erlaubt, immer größere Mengen unserer Daten abzugreifen und zu analysieren, kann auch freie Software davon profitieren.

Indem Moores Law weiterhin den Preis für Computergeräte senkt – seien es PCs, Smartphones oder Tablets – sind mehr Menschen in Entwicklungsländern auf der ganzen Welt in der Lage, sich diese zu leisten. Viele von ihnen werden freie Software benutzen, denn westliche Softwarefirmen verlangen oftmals übertrieben hohe Preise für ihre Produkte, wenn man sie mit dem lokalen verfügbaren Einkommen vergleicht.

Dadurch, dass Open Source sich weiter verbreitet, wird auch die Anzahl derer wachsen, die gewillt und fähig sind, etwas beizutragen. Die Software wird sich verbessern und mehr Menschen werden sie benutzen. Mit anderen Worten, es gibt einen selbstverstärkenden Kreislauf, der sich selbst nährt. Dieser wird dabei helfen, den sich immer

erweiternden Überwachungsaktivitäten von NSA und GCHQ entgegenzuwirken. Genauso wie Computer Werkzeuge von Repression sein können, können sie auch Werkzeuge des Widerstands sein, wenn sie mit freier Software betrieben werden, die ihren Namen nicht umsonst trägt.

Dieser Text wurde von der Redaktion ins Deutsche übersetzt.

Was Metadaten der NSA verraten

Wer seine Daten gezielt auf Webbrowser verteilt, hat gute Chancen, unter dem Radar der Überwachung durchzufliegen.

Erich Moechel

Die jüngsten, auf Edward Snowdens Unterlagen basierenden Enthüllungen über die globale NSA-Datenspionage sorgen nun in Lateinamerika für Schlagzeilen. Auch dort gilt das geheimdienstliche Interesse den ominösen Metadaten: Wer wann wo wie mit wem im Netz kommuniziert. Metadaten können zwar viel verraten, sind aber trügerisch.

Da die weitaus meisten dieser Verkehrsdaten aus Interaktionen von Websites mit den Webbrowsern entstehen, kommt dem Umgang mit dieser Alltagssoftware eine besondere Bedeutung zu. Über Cookies und Skripts wird nämlich nicht Kevin Normalbenutzer sondern sein Browser identifiziert. Würde Kevin seine Aktivitäten im Web allerdings auf zwei oder drei Browser verteilen, die noch dazu auf verschiedenen Geräten laufen, ergäbe das mehrere Profile, von denen keines besonders aussagekräftig wäre.

Doch Kevin macht das nicht, weil er den Internet Explorer nun einmal gewöhnt ist und obendrein sieht er gar keine Notwendigkeit, noch einen anderen Browser zu verwenden.

Metadaten und Profile

Die großen Profilersteller wie Facebook, Google und Co müssen nach wechselnden Vorgaben der NSA große Kontingente des Datenverkehrs auf Glasfaserschnittstellen kopieren, von wo sie die NSA mit eigenen Leitungen abtransportiert.

Hier werden die Profile abgesaugt, mitsamt den aktuellen Metadaten: Wann eingeloggt, wie lange, welche »Likes«, mit wem allem wie lang im Chat, welches Video wo verbreitet, wer hat wie darauf wie reagiert, wieviel GB Peer-to-Peer Datenaustausch mit wem, E-Mails usw.

Was Facebook und Google wissen

Auf diesem Weg hat Kevin Normalbenutzer mit seiner Sandra Kontakt gehalten, als er für seine Firma auf Montage in Saudi-Arabien war. Seitdem hat er auch ein paar neue Facebook- Freunde, die wie er im Maschinenbau tätig sind.

Sandra hat wiederum Kevin mit Videos vom kleinen Tim via Youtube auf dem Laufenden gehalten, die zugehörigen Metadaten sind in den Profilen Kevins und Sandras bei Facebook und Google aufbewahrt. Die Protokolle dieser Kommunikationen sind aber auch noch anderswo gelandet, weil die USA am Nahen Osten besonderes Interesse haben und die Datentransporteure obendrein noch Firmen aus den Vereinigten Staaten sind.

Das offizielle Europa zeigt sich angesichts der laufenden Enthüllungen über die Datenspionage der NSA ebenso ratlos wie im Jahre 2000 nach den Enthüllungen über das Echelon-System zur Funküberwachung der NSA.

Daten aus Saudi-Arabien

In den Datenzentren der weltweit führenden Betreiber von Glasfasernetzen, AT&T und Verizon, sind ebenfalls solche NSA-Schnittstellen vorhanden. In Kopie für die NSA werden dort Daten von den Geschäftskunden dieser US-Carrier bereitgestellt, das sind regionale Telekoms und Mobilfunker, die hier Bandbreite mieten. Kevin hat natürlich mit Sandra aus Saudi-Arabien regelmäßig telefoniert, auch diese Metadaten sind in den Sammlungen der US-Geheimdienste gelandet.

Wer die Metadaten eines Mobiltelefons über sechs Monate auswerten kann, erfährt um Zehnerpotenzen mehr über den Eigentümer, seine wichtigsten Kontaktpersonen und das soziale Umfeld, als eine altmodische Abhöraktion erbracht hätte.

Kritische Datenmengen

In Kombination mit Internet-Verkehrsdaten erschließen sich ab einer bestimmten, kritischen Datenmenge berufliche und private Kommunikation. Neigungen, Gewohnheiten und Motive treten so klar zu Tage, dass sich bereits Voraussagen über kommende Verhaltensweisen und Bewegungen ableiten lassen. Dieses »Profiling« macht jedes Individuum berechenbar, egal ob die Auswertung für die Geschäfte eines Internetkonzerns, die »nationale Sicherheit« oder für beides gleichzeitig geschieht.

So eindeutig wie sich die Situation darstellt, ist sie allerdings bei Weitem nicht. Das NSA-Modell basiert nämlich darauf, dass webbasierter E-Mail-Verkehr, Chats, webbasierte Telefonie, Dateiaustausch und Suchanfragen eben in erster Linie über Google, Microsoft, Facebook und Yahoo abgewickelt werden.

Der Browser als Verräter

Microsoft und Amazon pokern um die neuen, milliardenschweren Cloud-Aufträge der US-Militärgeheimdienste bereits mit. Ausgelagert werden vorerst Bürobetrieb und Verwaltung.

Dem Status Quo der NSA-Überwachung kommt entgegen, dass so ziemlich alle Benutzer ein- und denselben Webbrowser für alle Aktivitäten verwenden. Aus diesem Browser aber stammt nicht nur das Gros der Metadaten, dort werden sie auch miteinander verknüpft. Die von Facebook in Kevins Internet Explorer abgelegten »Cookies« registrieren, wenn Kevin eine Website mit eingebautem Facebook-Button abruft. Schon ist Kevins Interessensprofil bei Facebook um eine weitere Facette angereichert.

In einer anderen Datensammlung in den USA ist Kevins Facebook-Profil ebenfalls gespeichert, es ist allerdings dort mit einer Unzahl von anderen Metadaten verknüpft. Neben den Telefonaten aus Saudi-Arabien mit Firma und Familie sind da auch Kevins Youtube-Videos von nächtlichen Autorennen auf Wüstenpisten verknüpft. Kevin ist nämlich längst schon eine »Person of Interest« geworden, weil er für seinen Arbeitgeber davor schon einmal in Indonesien und in Bahrain auf Montage war.

Gaslieferungen und Eistüten

Die Gespräche über das geplante Freihandelsabkommen (TTIP) konnten nur deshalb am 8. Juli starten, weil die USA zugesagt haben, die EU-Delegationen diesmal nicht auszuspionieren.

Über Sandra ist hingegen kaum etwas bekannt. Sie benutzt Smartphone und iPad nur privat, weil sie damit auch gar nicht ins Virtual Private Network ihrer Firma käme. Seit Kevin zurück von seinem Montagejob ist, kann sie endlich wieder Vollzeit in der Anwaltskanzlei arbeiten. Dort wird sie auch dringend gebraucht, weil sie als einzige fließend Russisch spricht, was bei Geschäftsabschlüssen mit diesen Kunden ungemein hilfreich ist. In Sandras Profilen findet sich darüber so gut wie nichts und auch ihre Webbrowser hinterlassen keine Hinweise darauf, weil sich Sandra privat eben nicht für Erdgaslieferungen interessiert.

Das einzig Auffällige an Sandra ist, dass sie mit einem Techniker liiert ist, der beruflich schon mehrfach im Nahen Osten zu tun hatte. Für Kevins Firma ist das auch einer der wichtigsten Märkte, zumal dieses unscheinbare mittelständische Unternehmen aus Niederösterreich Weltmarktführer bei Teigrührmaschinen zur Produktion von Eistüten und Waffeln ist.

Dieser Text ist zuerst am 16. Juli 2013 auf ORF.at[259] *erschienen, wir Danken dem ORF sehr für diese Zweitverwertung.*

Wie NSA und GCHQ Verschlüsselung unterminieren

Das neueste, bekanntgewordene NSA-Projekt »Bullrun« sieht dem »Facebook-Überwachungsstandard« des European Telecom Standards Institute frappierend ähnlich.

Erich Moechel

»Verschlüsselung funktioniert. Sauber implementierte, starke kryptografische Systeme gehören zu den wenigen Dingen, auf die man sich verlassen kann«. Das war eine der ersten öffentlichen Aussagen Edward Snowdens direkt nach Ausbruch der Affäre.

Wie aber passt dies zu den jüngsten Enthüllungen von Guardian und New York Times, dass auch SSL-Verschlüsselung, Virtual Private Networks ebenso wie die Verschlüsselung der Blackberrys erfolgreich angegriffen wurden?

Die »aggressive und vielschichtige Herangehensweise der NSA während der letzten zehn Jahre« habe dazu geführt, dass »riesige Mengen verschlüsselter Internetdaten nunmehr ausgewertet werden« könnten, heißt es auf einer der Folien, die veröffentlicht wurden. Dazu hatte US-Geheimdienstkoordinator James R. Clapper wiederholt einen »Durchbruch bei der Entschlüsselungstechnologie« in den Raum gestellt.

Berechenbare Zufälle

Mit ziemlicher Sicherheit handelt es sich dabei um temporäre Schlüssel vor allem aus Mobilfunknetzen. Ebenso sicher lässt sich sagen, dass diese Schlüssel nicht geknackt, sondern zurückgerechnet wurden. Das wurde nur deshalb möglich, weil die zum Aushandeln eines temporären Schlüssels notwendigen Zufallszahlen nicht zufällig, sondern bekannt waren.

Im EU-Parlament hat am vergangenen Donnerstag das erste Hearing zum Überwachungsskandal stattgefunden, das nächste ist bereits für kommenden Donnerstag angesetzt.

Was nämlich bis jetzt über »Edgehill« und »Bullrun« bekannt wurde, ähnelt dem hier schon mehrfach als »Facebook-Überwachungstandard« und »Angriff auf die Blackberrys« beschriebenen Standardentwurf frappierend.

Dieser Normentwurf stammt aus dem European Telecom Standards Institute und läuft unter dem Titel »Cloud Lawful Interception«, gesetzmäßige Überwachung in der Cloud. Um das auch bei einer verschlüsselten Verbindung zu bewerkstelligen, muss sie angegriffen werden, während beide Endgeräte gerade einen temporären »Session Key« aushandeln.

»Deterministisch und monoton«

Die für diesen Vorgang erforderlichen Zufallszahlen sind aber keine, sondern »eine deterministische und monoton ansteigende Quantität, wie ein Zeitstempel oder ein externer Zähler«. So heißt es in einem 2011 bei einer Konferenz der ETSI-Arbeitsgruppe 3GPP SA3LI zur Überwachung der Mobilfunknetze vorgestellten technischen Ansatz.

Wenn der Netzbetreiber über denselben Generator von Pseudozufallszahlen verfüge wie die jeweilige Client-Anwendung – zum Beispiel ein Blackberry oder ein iPhone – dann sei es auf diese Weise seitens der Strafverfolger möglich, das »random secret« des jeweiligen Benutzers zu rekonstruieren. Damit ist die gesamte Kommunikation im Klartext verfolgbar, ohne dass der Schlüssel geknackt wurde.

Unterminierte Standards

Auch in den neuen, von Snowden veröffentlichten Dokumenten, finden sich Hinweise darauf, dass NSA/GCHQ die internationalen Standardisierungsgremien systematisch unterwandert haben, um die Entwicklung von Verschlüsselungssystemen zu unterminieren. Der Sekretär der zitierten Überwachungstruppe des European Telecom Standards Institute gehört der Einheit NTAC des britischen Militärgeheimdienstes GCHQ an.

Von dort stammt auch eines der ersten ETSI-Diskussionspapiere zum Thema Verschlüsselung, nämlich darüber, mit welcher Methode der Schlüsselaufbau angegriffen wird. Die britische Regierung habe ein ähnliches Schema entwickelt wie das derzeit im ETSI diskutierte, schreibt Ian Cooper, Sekretär von 3GPP SA3LI, in einem Diskussionspapier vom 7. September 2010.

»Niedrige Latenz«

In beiden Fällen wird das eigentlich sichere »Multimedia Internet KEYing« (MIKEY) zum Schlüsseltausch kompromittiert. Die britische Variante MIKEY-SAKKE sei der im ETSI diskutierten Methode MIKEY-IBAKE unter anderem durch »niedrige Latenz« überlegen.

Die beiden hier zitierten PDF-Dokumente enthalten noch eine Reihe weiterer Hinweise und werden deshalb hier zum »Peer-Review« zur Verfügung gestellt. Die »UK-Perspektive« ist tatsächlich die Perspektive des GCHQ.

Der wichtigste Unterschied dabei ist offenbar, dass die im ETSI lange favorisierte Methode zwar mehr Rechnerkapazitäten braucht, aber zumindest oberflächlich mit rechtsstaatlichen Grundsätzen in Einklang zu bringen ist. Die Verschlüsselung wird erst dann durch eine »Man in the Middle«-Attacke kompromittiert, wenn dazu ein Auftrag ergangen ist, etwa durch die Entscheidung eines ordentlichen Gerichts.

Durchbruch, aber »extrem fragil«

Die von Cooper gepriesene überlegen niedrige Latenz der britischen Methode aber beruht ganz offensichtlich darauf, dass alle Schlüssel sofort kompromittiert wurden, sobald sie erstmals im Netzwerk aufgetaucht sind und sofort »auf Halde« gespeichert werden.

Das GCHQ hatte diese Methode also Ende 2010 bereits operativ im Einsatz, zeitlich passt das genau zu den vom Guardian veröffentlichten Powerpoint-Folien, in denen der ominöse »Durchbruch bei der Entschlüsselung« allerdings technisch nicht näher ausgeführt wird.

Dafür finden sich allerdings Hinweise darauf, dass »Bullrun« als »extrem fragil« angesehen werden müsse, allein das Bekanntwerden des Programms könne schon genügen, dass »diese Möglichkeit schlagartig verloren ginge«. GCHQ und NSA sind für diese Programme nämlich vollständig auf die Komplizenschaft des Netzbetreibers angewiesen. Ohne die aktive Mitarbeit der Telekoms bzw. der Mobilfunker würde keines der zitierten, komplexen Überwachungsschemata funktionieren.

Aufwand

Der enorme Aufwand wiederum wäre nur dann nicht nötig, hätte die NSA etwa den als sicher geltenden, globalen Verschlüsselungsstandard AES 256 geknackt. Snowdens Aussage, dass man sich auf die Verschlüsselung selbst verlassen könne, passt also ganz genau ins Bild.

Der Zugang zu Informationen aus dem »Bullrun«-Programm ist strikt auf das GCHQ und seine »Partner zweiter Ordnung beschränkt«, das sind Australien, Neuseeland und Kanada. Dazu bedarf es noch einer speziellen »Clearance« für den Zugriff, die über Top Secret hinausgeht, nämlich »Bullrun indoctrinated«. Über letztere Qualifikation verfügte Edward Snowden offensichtlich nicht, andernfalls wären weit weniger Fragen noch offen.

Die exponentiell gestiegene Zahl von so akquirierten Schlüsselderivaten erklärt sich offenbar auch dadurch, dass diese Derivate des eigentlichen Schlüssels, der ganz anderswo, nämlich auf dem Keyserver eines Unternehmens liegt, periodisch erneuert werden müssen. Pro Benutzer fallen also regelmäßig neue, temporär gültige Schlüssel an.

Komplizenschaft

Damit wird auch verständlich, dass es sich um ein sehr aufwendiges System handelt, mit 250 Millionen kostet Bullrun mehr als das Zehnfache des vergleichsweise günstigen und trivialen »PRISM«-Systems.

Dass ein System wie »PRISM«, das von Microsoft bis Google die großen US-Internetfirmen verpflichtet, Kommunikationen der Benutzer für die

NSA/
GCHQ im Klartext zur Verfügung stellen, überhaupt gebraucht wird, ist ein klares Indiz dafür, dass auch diese scheinbar allmächtigen Geheimdienste weit davon entfernt sind, die gängigen, als sicher geltenden Algorithmen wie AES 256 quasi im Flug zu knacken.

Ohne direkte Komplizen unter den Telekoms und Internetfirmen, den Herstellern von Betriebssystemen für PCs, Smartphones usw. würde das derzeitige NSA-System schlichtweg nicht funktionieren.

Dieser Text ist zuerst am 9. September 2013 auf ORF.at[260] *erschienen, wir Danken dem ORF sehr für diese Zweitverwertung.*

Das Recht auf eigene Gerätehoheit als Bedingung der Privatsphäre

Erik Albers

Das Thema Überwachung dreht sich meist um die Überwachung des öffentlichen Raumes, spätestens seit PRISM auch um die der Telekommunikation. Im eigenen Zuhause oder im Kreise der Freunde hingegen denkt man nur selten an die Möglichkeit einer allgegenwärtigen Überwachung. Doch genau diese Gefahr droht durch den zunehmenden Kontrollverlust über unsere technischen (Kommunikations-)Geräte. Immer häufiger implementieren Hersteller Möglichkeiten des Fernzugriffs in ihre Produkte. Daraus resultierende Zugangs- und Kontrollmöglichkeiten seitens der Hersteller machen aus diesen Produkten zugleich willkommene Werkzeuge für Geheimdienste. Das persönliche Eigentum wird so zum Spion in der Tasche oder im eigenen Wohnzimmer. Um dieser Entwicklung entgegenzutreten bedarf es sowohl eines aufgeklärten Konsumverhaltens als auch eines aktiven Verbraucherschutzes, der dem Kunden die eigene Gerätehoheit garantiert.

Gerätehoheit besitzt derjenige, der die volle Kontrolle über die Hardware eines Computers ausübt und darüber bestimmt, welche Software dieser Computer auszuführen in der Lage ist und welche nicht. Als das ‘Recht auf eigene Gerätehoheit’ wird im Folgenden das Recht des Verbrauchers verstanden, die volle Kontrolle über die eigene Hardware auszuüben. Dies schließt die Verpflichtung der Hersteller ein, dem Verbraucher die eigene Kontrollausübung technisch auch zu ermöglichen. Dazu unabdingbar ist die freie Wahl darüber, welche Software die erstandene Hardware ausführt und – ebenso wichtig – welche nicht.

Obwohl sich das in Zukunft mit dem sogenannten ‘*trusted computing*’[261] ändern mag, waren Verbraucher diese Freiheit – die Freiheit, selbstständig über die verwendete Software des eigenen Computers zu entscheiden – bislang von klassischen Desktop- und Laptop-Computern gewohnt. Doch mit der zunehmenden Verbreitung weiterer Computer

im Alltag – Mobiltelefone, Navigationsgeräte, Spielekonsolen und Ähnliches – werden technische Geräte immer häufiger ohne entsprechende Hoheitsrechte an den Verbraucher ausgeliefert. Das Interesse der Hersteller ist dabei zunächst einmal von der Bindung des Kunden an das hauseigene Produkt geleitet, um auf dieser Basis fortführend Profite zu generieren. Bisherige Debatten um Gerätehoheit fokussierten sich deshalb oft auf Eigentums- und Verbraucherschutzrechte sowie marktwirtschaftliche und monopolrechtliche Bedenken. Spätestens seit den aktuellen Enthüllungen um das US-amerikanische Überwachungsprogramm PRISM jedoch muss die Debatte über die Gerätehoheit auch um das Recht auf Privatsphäre und den Schutz vor Überwachung erweitert werden. Denn mit dem Verlust der Kontrolle des Endnutzers steigen zugleich die Möglichkeiten einer Fernkontrolle durch den Hersteller. Die Fernkontrolle von Hardware bietet wiederum ein Eingangstor für Ausspähprogramme sowie andere Überwachungsmethoden moderner Geheimdienste.

Wie Hardware zum Spion werden kann

2013 hat Google ein Produkt namens *Google Glass* vorgestellt, ein Minicomputer im Design einer Brille – unter anderem ausgestattet mit Bildschirm, Internetzugang, Kamera, Mikrofon und GPS. Bereits die Ankündigung des Produktes hat eine Debatte über Sinn und Unsinn des Gerätes ausgelöst, die sich vornehmlich auf das Ausgeliefertsein derjenigen Person konzentriert hat, die vor der Brille steht. Denn steht mir jemand mit einer Brille gegenüber, die zugleich mit Kamera und Mikrofon ausgestattet ist – wie kann ich wissen, ob er mich nicht fotografiert, mich filmt oder unser Gespräch aufzeichnet? Wie kann ich wissen, wo er diese Daten speichert und wer dadurch sonst noch Zugriff auf all diese Daten hat? Wie kann ich mich fortan vor der Überwachung durch andere Personen schützen? So stellt die Fachzeitschrift *c't* in ihrem Langzeittest fest:

»Das ist das Grundproblem: Kein Mensch fühlt sich entspannt, wenn ein Objektiv auf ihn gerichtet ist. Beteuerungen, dass man auf keinen Fall fotografieren oder filmen will, helfen wenig – die Allgegenwart der Linse

verdirbt die Atmosphäre. Je häufiger man als Glass-Träger diese latente Unentspanntheit spürt, desto häufiger nimmt man die Brille ab. Am Ende will man sie nur noch aufsetzen, wenn gerade niemand in der Nähe ist.«[262]

So wichtig diese Debatte gesellschaftlich auch ist, so wurde einem anderen Aspekt leider viel zu wenig Aufmerksamkeit geschenkt: Der Möglichkeit von Google, das hauseigene Produkt ferngesteuert zu kontrollieren – mindestens, und das ganz offiziell, die Möglichkeit, die Brille ferngesteuert abzuschalten.

Glass Explorer Edition hieß die erste Version der Datenbrille, die von Google zum Betatest in limitierter Stückzahl an ausgewählte Personen ausgeliefert wurde. Diese mussten, um das Testprodukt nutzen zu dürfen, Googles Allgemeine Geschäftsbedingungen unterzeichnen, die unter anderem beinhalteten:

> *»Unless otherwise authorized by Google, you may only purchase one device, and you may not resell, rent, lease, transfer, or give your device to any other person. If you resell, rent, lease, transfer, or give your device to any other person without Google's authorization, Google reserves the right to deactivate the device, and neither you nor the unauthorized person using the device will be entitled to any refund, product support, or product warranty.«*[263]

Wenn Google folglich über die Möglichkeit verfügt, die eigene Datenbrille ferngesteuert auszuschalten, dann ist zu vermuten, dass sie auch weitere Möglichkeiten der Fernkontrolle beinhaltet – zum Beispiel das Aktivieren der Kamera oder des Mikrofons. Diese Form der Kontrolle und die Erfassung des privaten Alltags würde sich perfekt in Googles Geschäftskonzept integrieren: Die Sammlung möglichst vieler und möglichst genauer persönlicher Daten, um darauf basierend individuell zugeschnittene Werbung zu liefern. Technisch ist eine solche Fernkontrolle heutzutage ohne weiteres machbar.

Microsoft hatte vor wenigen Monaten mit der Ankündigung seines neuesten Produktes *Xbox One* schon ähnliche Kontrollphantasien

vermuten lassen. Die *Xbox One* ist eine Spielekonsole, deren technische Spezifikationen sich bereits wie ein High-End Spionageprodukt lesen: Full HD Kamera mit biometrischem Scan, Emotionserkennung sowie Standortbestimmung, eine Nachtsicht- und Infrarotfunktion sowie vier Mikrofone mit individueller Stimmerkennung, die per se nicht ausgeschaltet werden können. Hinzu kündigte Microsoft an, dass ein beständiger Datenaustausch zwischen der *Xbox One* und den Microsoft Servern für die Übermittlung personalisierter Werbung bestehen werde. Erst nach einem Sturm der Entrüstung von Kunden und Datenschützern ist Microsoft inzwischen zurückgerudert – sonst wäre die *Xbox One* der perfekte Spion im eigenen Wohnzimmer geworden. Schließlich ist es ein einfacher Schritt, in ein Gerät, das in beständigem Datenaustausch steht, auch die Möglichkeit einer Fernkontrolle zu implementieren.

Wenn sich aber moderne IT-Produkte durch deren Hersteller individuell fernsteuern lassen, dann ist dies zugleich eine Eintrittstür für die amerikanische National Security Agency (NSA) oder andere Geheimdienste. Laut dem Guardian – in Berufung auf die Enthüllungen von Edward Snowden – wird der NSA seit 2007 direkter Zugriff auf die Daten und in die Systeme Microsofts ermöglicht und seit 2009 auch auf diejenigen Googles[264]. Selbst wenn es stimmen sollte, dass derartige Zugriffe der NSA nur äußerst selektiv erfolgen, stellt die Herausgabe von Zugangsdaten, die der Fernkontrolle von Hardware dienen, seitens der Hersteller ein nahezu perfektes Überwachungsinstrument und damit einen tiefgreifenden Eingriff in das informationelle Selbstbestimmungsrecht jedes Einzelnen dar. Die eigene Gerätehoheit wird so zur Voraussetzung für den Schutz der eigenen Privatsphäre.

Lösung: 'Control by Design'

Der Zusammenhang von Gerätehoheit und Privatsphäre ist von zentraler Bedeutung. Das Argument, dass keiner gezwungen sei, derartige Produkte zu kaufen, wird zukünftigen Entwicklungen nicht länger gerecht. Zwar kann man anhand der genannten Beispiele behaupten, dass niemand ein *Google Glass* oder eine Microsoft *Xbox One* kaufen müsse. Doch findet sich ähnliche Hardware bereits heute in

unzähligen Gegenständen, auf die man weder in der Arbeitswelt noch im privaten Alltag verzichten kann, wie beispielsweise Laptops oder Mobiltelefone. Auch bedarf es keiner großen Vorstellungskraft mehr, um zu sehen, dass wir in naher Zukunft von immer mehr Geräten umgeben sein werden, die mit gleicher Hardware ausgestattet sind[265]. Was deshalb heute für die Kontrolle unserer Kommunikationsgeräte oder der oben genannten Datenbrille und Spielekonsole gilt, wird in Zukunft für immer mehr Dinge gelten: Uhren, Wecker, Kopfhörer, Kaffeemaschinen, Kühlschränke und die meisten technischen Geräte werden in Zukunft die Möglichkeit haben, über das Internet Daten auszutauschen. Zwar werden nicht alle diese Geräte als Überwachungsmaschine dienlich sein, weil ihnen Augen und Ohren – beziehungsweise Kamera und Mikrofon – fehlen. Doch auch die Geräte, die nicht mit derlei Hardware ausgestattet sind, werden Daten produzieren, deren Analyse immer präzisere Formen der individuellen Kontrolle und Überwachung ermöglicht. Der Kühlschrank zum Beispiel: Auf den ersten Blick erscheint dessen Inhalt nicht zentral für die Privatsphäre zu sein. Doch lassen sich auch dadurch Rückschlüsse auf unser Konsumverhalten (z.B. Vegetarismus), unsere Gesundheit (z.B. Medizin), unser Wohlbefinden (z.B. Alkoholkonsum) oder unsere körperliche Anwesenheit (z.B. Veränderung bzw. Nicht-Veränderung des Inhalts) schließen.

Privatsphäre und die Möglichkeit der privaten Kommunikation sind jedoch Voraussetzungen für eine freie Gesellschaft, die wiederum Voraussetzung für ein freies demokratisches Gemeinwesen ist. Um diese Freiheiten zu wahren, muss deshalb für alle Geräte mit Internetzugang – in Anlehnung an die Forderung nach einem '*Privacy by Design*'[266] – ein Konsens über ein '*Control by Design*' etabliert werden: Ein Ansatz, in dem bereits bei der Entwicklung neuer Hardware-Produkte die *eigene Gerätehoheit* in die Gesamtkonzeption einbezogen, eingehalten und geprüft werden muss. Denn um seinem Recht auf Privatsphäre gerecht zu werden, muss ein Nutzer jederzeit in der Lage sein, seine eigene Hardware abzuschalten und eigenständig darüber bestimmen zu können, wann beispielsweise eine Kamera oder ein Mikrofon aktiv ist.

Genauso muss ein Nutzer darüber entscheiden können, wann welche Daten eines Gerätes wohin übertragen werden. Eine unautorisierte Fernkontrolle hingegegen muss ausgeschlossen sein. Letztendlich sind diese Forderungen nur realisierbar, wenn wir auch die Kontrolle über die Software haben, die wir zur Kontrolle der Hardware verwenden. Erst das Recht, jede Software auf jedem Gerät zu installieren, beziehungsweise zu entfernen, ermöglicht uns die volle Gerätehoheit.

Für das »Internet der Dinge« muss schließlich das gleiche gelten, was heutzutage noch für das *World Wide Web* gilt: Die Möglichkeit der Teilhabe für Jedermann unter vollständiger Kontrolle seiner verwendeten Hardware. Ebenso muss die Möglichkeit zur Verwendung freier Software garantiert sein. Um das zu ermöglichen, benötigen wir ein umfassendes Recht auf die eigene Gerätehoheit.

Technologie in die Hände der Gesellschaft

Wirtschaft, Staat und Geheimdienste haben, wenn auch aus unterschiedlichen Motiven, gemeinsam das Interesse an möglichst detaillierten Informationen über die einzelnen Individuen unserer Gesellschaft – die Wirtschaft aus ökonomischen Interessen und der Staat sowie dessen Apparate aus dem Interesse an einem vermeintlichen Sicherheitsgefühl. Die Kontrolle der Technologie wird dabei zu einem zentralen Element, das imstande ist, unsere Privatsphäre auszuhöhlen. Diesen Kontrollverlust des Verbrauchers zu unterbinden wird zu einer wichtigen Aufgabe für Gesellschaft und Politik. Oder, wie Joseph Weizenbaum es einst ausdrückte: »Daß die Menschheit in diesem höchst instabilen und gefährlichen Zustand lebt und abhängig ist von einer Technik, die sie kaum noch durchschaut, ist keine zwangsläufige Folge der technischen und wissenschaftlichen Entwicklung – es ist eine Folge des moralischen und politischen Entwicklungsstandes der Gesellschaft.«[267]

Um dem Kontrollverlust der Gesellschaft und des Einzelnen entgegenzutreten, sind unterschiedliche Wege denkbar. Elementar ist das Verbot jeglicher unautorisierter Form der Fernkontrolle und Zugriffsmöglichkeit sowie die Garantie und das Recht auf die eigene

Gerätehoheit. Damit wäre es – je nach Komplexität des Gegenstandes – zumindest für technisch versierte Personen möglich, der Überwachung und Kontrolle durch Dritte zu entgehen. Um jedoch auch den technisch weniger versierten Verbraucher bestmöglich zu schützen und Aufklärungsarbeit zu leisten, sind weitere Formen des Verbraucherschutzes nötig. Längst überfällig ist beispielsweise eine Kennzeichnungspflicht für Hardware. Ähnlich wie auch Nahrungsmittelhersteller auf ihre Inhaltsstoffe und Zutaten hinzuweisen haben sollten auch Hardwarehersteller verpflichtet werden, ihre Kunden auf Einschränkungen oder Kontrollmöglichkeiten der Hardware hinzuweisen. Zum Beispiel »*Dieses Produkt kann nicht offline genutzt werden*«, »*Dieses Produkt steht in ständigem Datenaustausch mit Firma XY*«, »*Dieses Produkt verwendet Ihre persönlichen Daten zur Bereitstellung personalisierter Werbung*«, »*Dieses Produkt hat Kamera und Mikrofon dauerhaft aktiviert*« und so weiter. Eine derartige Kennzeichnungspflicht würde dem Verbraucher nicht nur die Einschränkung seiner Privatsphäre deutlich machen, sondern ihm dadurch erst die Möglichkeit geben, eine informierte und aufgeklärte Entscheidung zu treffen.

Schwachstellen bei dieser Form der Selbstregulierung verblieben jedoch in der Überprüfung der gemachten Angaben. Denn während die Kontrolle eines Lebensmittels auf dessen Inhaltsstoffe möglich ist, ist die Überpüfung geschlossener IT-Systeme und geschlossener Quellcodes kaum möglich. Wie könnte man also die Angaben der Hersteller verifizieren? In der Theorie wäre dazu eine Prüfstelle denkbar, welcher komplette Einsicht in die verwendete Hardware und Software gegeben werden müsste. Damit könnten bestehende Einschränkungen oder Kontrollmöglichkeiten entdeckt werden. In der Praxis scheint ein solches Vorhaben jedoch allein aufgrund der unübersichtlichen Anzahl der monatlich neu erscheinenden technischen Geräte, den damit verbundenen langen Prüfzeiten, sowie fehlender internationaler Standards und Gremien unrealisierbar. Die effektivste Lösung ist daher die Einführung des allgemeinen Rechts jeden Verbrauchers, jede Software auf dem eigenen Gerät installieren zu dürfen und die Möglichkeit, vorhandene Software vollständig deinstallieren zu können.

Indem die Möglichkeit gegeben ist, eigene Software zu verwenden, ist niemand länger auf die Software des Herstellers angewiesen. Dann kann jeder Kunde für sich entscheiden, ob er der Software des Herstellers vertraut oder nicht.

Auf lange Sicht wäre es zielführend zum Schutz der Privatsphäre, Hersteller zu verpflichten, ihre Software offenzulegen. Auch wenn der Quellcode nicht als Freie Software veröffentlicht wird, würde seine Offenlegung zumindest die Überprüfung der Software durch Jedermann ermöglichen. Damit könnten Gefahren von Hintertüren und versteckter Fernkontrolle durch die Softwarehersteller weitestgehend ausgeschlossen oder zumindest transparent gemacht werden. Die Kontrolle und Hoheit über technische Geräte und deren verwendete Software würde dadurch direkt in die Hände des Verbrauchers und damit in die Hände der Gesellschaft gegeben werden. Damit es soweit kommen kann, ist es wichtig, ein allgemeines Bewusstsein über die Bedeutung des Rechts auf die eigene Gerätehoheit zu schaffen und auf diesem Recht zu beharren. Nur so kann erreicht werden, dass zukünftige Technologien – statt unserer Überwachung zu dienen – unserer eigenen Kontrolle unterliegen werden.

Neue Geheimdienstrechenzentren in den USA

Moritz Tremmel

Anfang 2012 wurde der Bau des NSA-Rechenzentrums in Utah bekannt – ein monströses Rechenzentrum für die NSA-Datenverarbeitung. Schon ein Jahr später im März 2013 wurde ein weiteres geheimdienstliches Rechenzentrum in den USA in Auftrag gegeben[268]. Dieses steht in unmittelbarer Nähe zum Sitz des Überwachungsgeheimdienstes National Security Agency (NSA) und dem Militärgeheimdienst Defense Information Systems Agency (DISA) in Fort Meade, Maryland. Das 565 Millionen Dollar teure »Hochleistungsrechenzentrum« soll von Militärgeheimdiensten betrieben werden und bereits 2015 in Vollbetrieb gehen.

Das neue Rechenzentrum in Fort Meade, einem Städtchen, dessen gesamte Infrastruktur von der NSA kontrolliert wird, dient vor allem der Absicherung von Militärkommunikation und ist wohl eine Reaktion auf Wikileaks und Whistleblower wie Bradley Manning. Bisher hatten mindestens zwei Millionen Menschen Vollzugriff auf den militärischen Datenpool SIPRnet (Betreiber DISA) und konnten ohne Routinen zur Plausibilitätsprüfung alle Daten abfragen und downloaden.

Das schon länger bekannte NSA-Rechenzentrum in Utah[269], das im September 2013 seinen Betrieb aufgenommen hat, hingegen dient der Überwachung von (Internet-)Kommunikation. Die Aufgabe des neuen Rechenzentrums ist es, die u.a. über Satelliten, Überseekabel oder zentrale US-Switches der Telekommunikationsanbieter im großen Stil abgefangenen Daten zu analysieren, zu speichern und zu entschlüsseln. Laut einer Aussage des Journalisten und NSA-Experten James Bamford sei der Bedarf an Rechenleistung in den letzten Jahren abrupt gestiegen, seit die NSA eine weltweit verwendete Verschlüsselungsmethode knacken könne.

Spekulationen und Enthüllungen über Entschlüsselung

Seither wird spekuliert, welcher Verschlüsselungsalgorithmus damit gemeint sein könnte: Gemunkelt wird vor allem über AES (Advanced Encryption Standard) und RSA. Beide Verschlüsselungsstandards sind weit verbreitet und werden tagtäglich eingesetzt um beispielsweise sichere Verbindungen zu Webseiten oder Webservern via SSL und TLS aufzubauen oder werden bei PGP und GnuPG meist zur Verschlüsselung von E-Mails eingesetzt.

Der Kryptografieexperte Bruce Schneier geht nicht davon aus, dass die NSA den Verschlüsselungsstandard AES brechen kann. Allerdings könne die NSA sehr wohl über andere Angriffsvektoren an den mit AES verschlüsselten Inhalt kommen. Als Beispiele nennt er Side-Channel-Attacks, Attacks against the Key Generation Systems (z.B. über schlechte Zufallszahlengeneratoren), schlechte Implementierungen des Verschlüsselungsstandards oder einfach das Anzapfen der Computer, auf denen die Verschlüsselung stattfindet. Eine andere Möglichkeit in Bezug auf RSA-1024 bestünde laut Schneier darin, dass die NSA Hardware entwickelt haben könnte, die eine Faktorzerlegung von 1024-Bit beherrscht[270].

Die von Edward Snowden geleakten Dokumente untermauern die These von Bruce Schneier. Die NSA und der britische Geheimdienst GCHQ betreiben Programme, die Verschlüsselung aufheben sollen. Bullrun (NSA) und Edgehill (GCHQ) sind teure, ausgefeilte Programme, die aber nicht die Verschlüsselungsalgorithmen selbst angreifen, sondern die Verschlüsselung auf Umwegen aushebeln. In kommerzielle (Verschlüsselungs-)Programme werden Hintertüren eingebaut, Standardisierungsgremien werden unterwandert und beeinflusst, häufig wird auch einfach versucht durch Druck oder Hacking an die Masterkeys, also die geheimen Schlüssel über die die Kommunikationsverschlüsselung abgewickelt wird, zu gelangen.

Nicht wenige Umsetzungen der kryptografischen Standards haben ein Problem: Sie sind nicht sauber umgesetzt. Wird beispielsweise ein schlechter Zufallszahlengenerator verwendet lassen sich die Schlüssel zurückrechnen und die Kryptografie lässt sich knacken – ohne dass der

eigentliche Verschlüsselungsstandard gebrochen wurde. Genau hier setzen Geheimdienste wie die NSA an. Der enorme Aufwand, der hier betrieben wird, wäre wohl kaum notwendig, könnte die NSA gängige Verschlüsselungsstandards brechen[271].

Da passt die Aussage von Edward Snowden direkt nach dem Ausbruch des Skandals gut ins Bild: »Verschlüsselung funktioniert. Sauber implementierte, starke kryptografische Systeme gehören zu den wenigen Dingen, auf die man sich verlassen kann.«

Das zukünftige Rechenzentrum für PRISM

Ein anderer Grund für den gewachsenen Rechen- und Speicherbedarf sind Programme wie PRISM, bei welchem massenhaft Daten von großen Internet- und Telekommunikationsfirmen wie Google, Facebook, Yahoo, Microsoft/Skype und anderen abgeschnorchelt werden. Um die Daten speichern und auswerten zu können, braucht die NSA immer größere Rechen- und Speicherkapazitäten. Das zwei Milliarden Dollar teure Rechenzentrum in Utah bietet massenhaft Speicher und Rechenpower dafür – und bringt das Pentagon näher an ihr 2007 geäußertes Fernziel, Daten im Yottabyte-Bereich verarbeiten zu können. Zum Vergleich: Zwischen 2010 und 2015 soll sich, laut einer Studie von Cisco, der globale Internettraffic auf 966 Exabyte pro Jahr vervierfachen. Sprich 2015 beträgt der globale Internettraffic knapp 1 Zettabyte (1000 Exabyte), das wiederum nur ein Tausendstel von der geplanten Kapazität eines Yottabytes ist. Ein Yottabyte umfasst in etwa 500 Trillionen (500.000.000.000.000.000.000) Seiten Text[272].

Um die Datenmengen speichern zu können umfasst das Rechenzentrum in Utah vier Hallen mit je 2.300 Quadratmetern Raum für Server. Allein die Stromkosten sollen 40 Millionen Dollar pro Jahr betragen.

Noch mehr Rechenzentren und Supercomputer

Das Rechenzentrum in Utah ist aber mitnichten der einzige Ort, an dem die NSA Daten speichert oder auswertet – es ist nur das momentan (!) größte Rechenzentrum des Geheimdienstes:

- Vier NSA-Satelliten können von Walkie-Talkie- über Mobiltelefongespäche bis hin zu Radar-Systemen alles abfangen. Diese Daten werden schon im Satelliten vorgefiltert, der Rest landet auf den Schreibtischen der 850 NSA-Mitarbeiter in der Aerospace Data Facility, Buckley Air Force Base, Colorado.
- Die Kommunikation aus Europa, dem Nahen Osten und Nordafrika wird in Fort Gordon, Augusta, Georgia von 4.000 Analysten bearbeitet.
- Die Daten aus Lateinamerika landen auf der Lackland Air Force Base, San Antonio in Texas – seit dem 11. September werden hier von den 2.000 NSA-Mitarbeitern auch Daten aus dem Nahen Osten und Europa analysiert. Das dortige Rechenzentrum wurde erst jüngst für 100 Millionen Dollar renoviert und ist eine Art Backup für das Rechenzentrum in Utah.
- Auf Hawaii kommen vor allem die Daten aus dem asiatischen Raum an – hier arbeiten 2.700 Menschen.
- Im Multiprogram Research Facility, Oak Ridge, Tennessee arbeiten 300 Wissenschaftler und Computerspezialisten vor allem an der Kryptoanalyse und anderen geheimen Projekten – hier steht einer der schnellsten Supercomputer der Welt.
- Und natürlich nicht zu vergessen die Zentrale der NSA in Fort Meade, Maryland – auch hier soll ein 896 Millionen Dollar teurer Supercomputer gebaut werden um den immer weiter steigenden Datenmengen Herr werden zu können.

Das Ziel all dieser Orte fasst ein NSA-Beamter gegenüber dem Wired-Magazin[273] gut zusammen: *Everybody's a target; everybody with communication is a target.*

Kryptographie nach Snowden

Prof.Dr.rer. nat. Rüdiger Weis

Nach den Enthüllungen von Edward Snowden müssen viele kryptographische Anwendungen einer Neubewertung zugeführt werden. Die gute Nachricht ist, dass wissenschaftlich starke Kryptographie auch für übermächtige Geheimdienste nicht brechbar sein dürfte.

Allerdings sollten zukünftig Warnungen aus der Wissenschaft ernst genommen werden. Starke Kryptographie sollte als Standardeinstellung benutzt und im klugen Ingenieurssinne ausreichend große Sicherheitsspielräume, sprich bewährte Algorithmen mit langen Schlüssellängen, gewählt werden.

Die jetzt bestätigten geheimen Einbauten von Hintertüren durch US-Firmen führen ein weiteres Mal die Notwendigkeit für eine neue Vertrauensbasis für die digitale Welt vor Augen. Hierfür sind Schlüsselkontrolle durch den Anwender, nachvollziehbare Standardisierungsprozesse und einsehbarer Sourcecode für Software und Hardware als unabdingbar anzusehen.

Mathematik hilft den Schwachen

> *»Trust the math. Encryption is your friend.«*
>
> *– Bruce Schneier, Guardian, 6. September 2013.*

Kryptographische Algorithmen gehören zu einer Königsdisziplin der Mathematik. Die meist zugrunde liegende Zahlentheorie galt über die Jahrhunderte als eines der schwierigsten und reinsten Wissensfelder der Mathematik. In der Vor-Computerzeit meinten viele Mathematiker dies durchaus im Sinne von »nicht mit realer Anwendbarkeit beschmutzt«.

Gründlich irrten sich hier kluge Menschen, Kryptographie ist zur zentralen Technologien der digitalen Welt geworden und eine der wenigen Technologien, bei der Beschleunigung den Schwachen hilft. Die

immer schneller werdenden Systeme bevorteilen in mathematisch nachweisbarer Weise den Verschlüsselnden gegen den Angreifer.

Kryptographie ermöglicht durch Mathematik auf einer kleinerfingernagelgroßen Fläche oder in mit einer handvoll Programmzeilen, Daten sicher selbst gegen eine weltweite Geheimdienstzusammenarbeit zu verschlüsseln. Freie Software ermöglicht dies kosten- und hintertürenfrei.

Pessimisten meinen, dass Kryptographie die letzte Brandmauer gegen eine umfassende Überwachung darstellen könnte, die allerdings in der Praxis häufig umgangen werden kann. Optimisten glauben, dass Kryptographie zu einer Stärkung des Einzelnen gegenüber den Staaten führt und damit eine wichtige Befreiungstechnologie darstellt.

Nicht stärkste Kryptographie ist schwach.

Die geringe Aufgeregtheit in der kryptographischen Forschung nach den Enthüllungen rührt daher, dass man seit jeher nur kosmische Konstanten als Grenze der Mächtigkeit des Angreifers für diskussionswürdig hielt. Konkret rechnet man schon immer mit einem Angreifer, der alle Nachrichten abhören kann und Milliarden Dollar zum Brechen der Verschlüsselung zur Verfügung hat.

Nach Snowden wissen wir genauer, an welchen Kabelstellen abgehört wird und auf den Cent genau, wie viel Geld für Kryptoangriffe vorhanden ist. Nicht uninteressant, aber wissenschaftlich betrachtet nur eine Fußnote.

Die »übertriebene Paranoia« der Theoretiker hat sich also mal wieder als die realistischste Einschätzung der praktischen Bedrohungslage erwiesen.

Nach Snowden ist es sicher, dass kryptographische Verfahren, gegen die akademische Vorbehalte bestanden, wohl auch praktisch gegen mit Milliarden ausgestattete Gegner mehr als problematisch sind.

Kaputt: RC4, SHA1 und RSA-1024

Zentrale Sicherheitsbausteine des, eine sicher Web-Kommunikation garantierenden, TLS(SSL)-Protokols sind symmetrische, asymmetrische

Verfahren und Hashfunktionen. In allen drei Bereichen müssen höhere Sicherheitsanforderungen gestellt werden.

Nicht mehr verwendet werden sollte die bei TLS häufig als Standard verwendete RC4-Stromchiffre. RC4 ist ein Geniestreich von Ron Rivest. Es ist unglaublich elegant, schnell, mit wenigen Progammzeilen und sogar mit Spielkarten implementierbar. Die Kryptographieforscher stehen allerdings nicht nur mit ehrlicher Bewunderung vor einem derart schönen Algorithmus, er weckt natürlich auch den Ehrgeiz der Angreifer.

Das Verfahren ist ganz anders konstruiert als gängige Algorithmen und deshalb können neue Angriffe einen Totalschaden herbeiführen, was bei alten, langweiligen Verfahren sehr unrealistisch erscheint.

Nach Snowden können wir, insbesondere dank der Informationen zu Tor-Angriffen, davon ausgehen, dass die NSA hier vor wenigen Jahren einen Durchbruch erreichen konnte.

Ähnlich düster sieht die Lage bei Hashfunktionen aus. Hashfunktionen sind wichtige Bausteine von kryptographischen Systemen, denen bisher relative geringe Aufmerksamkeit gewidmet wurden. Dies ist auch deshalb überraschend, da Schwächen von Hashfunktionen beispielsweise für das Fälschen von Zertifikaten ausgenutzt werden können, selbst wenn die eigentliche Signaturfunktion sicher ist.

Hier gab es in der öffentlichen Forschung einige dramatische Durchbrüche. Fast alle in Anwendung befindlichen Hashfunktionen stammen von Ron Rivests MD4-Hashfunktion ab. Gegen MD4 gab es schon früh Sicherheitsbedenken, MD5 und SHA ergänzten Operationen zur Erhöhung der Sicherheit. MD4 ist inzwischen mit Bleistift und Papier brechbar. MD5 und SHA sind ebenfalls schon mit überschaubarem Aufwand angreifbar.

Eine Analyse von Stuxnet ergab, dass die NSA über Techniken zum Angriff auf die MD4-basierte Hashfunktionen-Familie verfügt, die in der öffentlichen Forschung bisher nicht bekannt waren.

Auch das inzwischen angewendete und bisher noch nicht gebrochene SHA2-Verfahren stammt aus dem Hause der NSA und ist ähnlich konstruiert. Das neue Hashverfahren SHA3 wurde in einem offenen transparenten Wettbewerb ausgewählt und ist bewusst völlig anders konstruiert.

Im Bereich der Public-Key-Kryptographie halten führende Kryptographen schon seit vielen Jahren RSA mit einer Schlüssellänge von 1024 Bit für brechbar. Die Behörden verpflichten schon seit längerem eine Mindestlänge von 2048 Bit und halten längere Schlüssellängen schon mittelfristig für empfehlenswert. Viele Kryptographieforscher empfehlen mindestens 4096 Bit.

Der laufende Wechsel zu Elliptischen Kurven Kryptosystemen (ECC) bringt eine Reihe von theoretischen und praktischen Gefahren mit sich.

Problemfall Elliptische Kurven

Eine der interessantesten Entwicklungen im Bereich der Kryptographie ist die verstärkte Nutzung von Elliptischen Kurven Kryptosystemen. Die Hauptidee hierbei ist, das schon lange bekannte Diskrete Logarithmus Problem (DLP) auf mathematisch anspruchsvollen Strukturen zu verwenden.

Das DLP wurde schon in der Vorcomputerzeit theoretisch eingehend untersucht und war auch die Grundlage für das erste praktisch nutzbare Public-Key-System von Whitfield Diffie und Martin Hellman. Anschaulich gesprochen basiert es auf der schon mit Schulmathematik nachvollziehbaren Beobachtung, dass es sehr viel einfacher ist, zu Exponenzieren als einen Logarithmus zu berechnen. Die neue Idee war nun, diese Beobachtung für ähnliche Strukturen auf mathematischen Kurven zu untersuchen. Hierbei verwendet man statt einer normalen Multiplikation von ganzen Zahlen mit anschließender Restbildung eine geometrisch motivierte Addition von Punkten.

Die Mehrheit der kryptographischen Forschung ist der Ansicht, dass ECC ähnliche Sicherheit liefert wie gängige Verfahren wie RSA bei deutlich kürzeren Schlüsseln und damit bessere Performance. Diese

Eigenschaften sind besonders im Bereich Smartcards und eingebettete Systeme bedeutend.

Eine Minderheit der Kryptographen kritisiert, dass man im Wesentlichen lediglich weiß, dass der gegen DLP-Systeme über endlichen Körpern sehr wirkungsvolle Index-Calculus Angriff nicht unmittelbar gegen das DLP über der additiven Gruppe von Elliptischen Kurven angewendet werden kann. Gerade die reichhaltige algebraische Struktur von Elliptischen Kurven könnte sehr überraschende und wirkungsvolle Angriffe möglich machen.

Zudem ist ECC wegen der kürzeren Schlüssellänge viel anfälliger gegen Angriffe mit Quantencomputern (Shor-Algorithmus).

Nach Snowden wissen wir centgenau, dass die NSA erhebliche Mittel in die Forschung zu Quantencomputern steckt.

NSA ECC-Parameter

Ein erhebliches praktisches Problem stellt weiterhin die Tatsache dar, dass ECC-Systeme eine Reihe von mathematisch höchst sensiblen Parametern benötigen. So wurde von offen forschenden Kryptographen in einem NIST-Standard schon im Juni 2006 die hohe Wahrscheinlichkeit einer Manipulation von Elliptische-Kurven-Parametern für einen Zufallsgenerator (Dual Elliptic Curve Deterministic Random Bit Generator) aufgedeckt.

Nach Snowden bestätigt sich die Existenz einer NSA-Backdoor in einem NIST-Standard. Der Vertrauensverlust der Standardisierungsbehörde ist ein harter Schlag für die Informatik.

Implementierungsproblem Zufallszahlen

Es bestehen zusätzlich auch einige strukturelle Probleme von ECC-Systemen. Die weit verwendeten ECC-Systeme basieren auf dem Diskreten Logarithmus Problem. DLP-Systeme brauchen bei jeder Signatur starken Zufall. Wenn man für zwei Nachrichten den selben Zufallswert verwendet, wird der Schlüssel kompromittiert und kann durch einfache Umformungen aus der Schulmathematik direkt

ausgerechnet werden. Ein manipulierter Zufallsgenerator führt direkt zum kryptographischen Super-GAU.

Nach Snowden haben wir es schriftlich, dass gerade ECC-Parameter und Zufallsgeneratoren offensichtlich zu den NSA-Lieblingsangriffszielen gehören

Viele Kryptographen sehen unter anderem daher inzwischen die Probleme von ECC-Systemen als erheblich und empfehlen die konservative Verwendung von RSA mit großer Schlüssellänge.

Problemfall Trusted Computing

> *»Privacy tends to go down in inverse*
> *to the number of transistors in the world.«*

– Ron Rivest

Neu bewertet werden muss auch die Initiative vom Microsoft und befreundeten Firmen, den Nutzern eine neue Sicherheitsarchitektur namens Trusted Computing aufzuzwingen. Hierbei soll ein Trusted Computing Modul (TPM) in die persönlichen Computer und Mobilgeräte eingebaut werden. Dieses enthält einen Schlüssel, auf den der Besitzer des Computer keinen Zugriffs hat. Zusammen mit den nun von Microsoft implementierten Verfahren innerhalb von Windows 8 (insbesondere Secure Boot) wird dem Nutzer weitgehend die Kontrolle über seine eigene Hardware und Software entzogen.

Es erinnert fatal an eine elektronische Fußfessel. So kann beispielsweise über das Netz angefragt werden, ob nur genehmigte Software läuft. Das Ende der persönlichen Computer und Smartphones. Es klingt wie ein Traum für außer Kontrolle geratene Geheimdienste und repressive Staaten.

Whitfield Diffie, einer der Entdecker der Public-Key-Kryptographie, zeigte sich besorgt über die dominierende Stellung von Microsoft und forderte, dass die Benutzer die vollständige Kontrolle über die Schlüssel des eigenen Computers behalten sollten:

> *»(The Microsoft approach) lends itself to market domination,*
> *lock out, and not really owning your own computer.«*
>
> *»To risk sloganeering,*
> *I say you need to hold the keys to your own computer.«*

Auch Ron Rivest mahnte eindringlich, die möglichen Konsequenzen gründlich abzuwägen:

> *»We should be watching this to make sure*
> *there are the proper levels of support we really do want.«*
>
> *»We need to understand the full implications of this architecture.*
> *This stuff may slip quietly onto people's desktops,*
> *but I suspect it will be more a case of a lot of debate.«*

Das TPM ist ein Dream Chip für die NSA. Wenn Wirtschaft und Behörden mittels Windows und Trusted Computing eine Sicherheitsinfrastruktur aufbauen, können die US-Behörden im Zweifelsfall die völlige Kontrolle übernehmen.

Angesichts der Tatsache, dass wiederholt Druck auf Hardwarehersteller ausgeübt wurde, Hintertüren einzubauen, wirkt die Idee, dass ein Schlüssel vom Benutzer nicht ersetzt werden kann, sehr bedrohlich. Besonders brisant ist, dass die geheimen Schlüssel während des Herstellungsprozesses außerhalb des Chips erzeugt und danach in den Chip übertragen werden. Hier ist es trivial, eine Kopie aller Schlüssel herzustellen. Es ist nicht auszuschließen, dass entsprechende Rechtsvorschriften bestehen und über diese nicht berichtet werden darf.

Zwar besteht die Hoffnung, dass die USA als demokratischer Rechtsstaat hier Änderungen durchführen wird. Im Kongress wurde 2013 eine stärkere Geheimdienstkontrolle nur sehr knapp abgelehnt. Trotzdem ist die im Moment bestehende Rechtslage hier völlig unakzeptabel. Das andere realistische Szenario, dass der TPM-Hersteller nicht in der Reichweite der NSA sondern in China sitzt, kann nicht wirklich beruhigen.

Da neben den Überwachungsmöglichkeiten auch die Programmauswahl der Nutzer behindert wird, stellen sich natürlich kartell- und verbraucherrechtliche Fragen. Unter anderem die Tatsache, dass Microsoft die übliche Praxis verlassen hat und den Überwachungschip automatisch einschaltet und faktisch nicht mehr ausschalten lässt, verstößt unter anderem gegen das Eckpunktepapier des Bundesinnenministeriums zur vertrauenswürdigen Technikgestaltung.

Hintertüren in Closed Source Soft- und Hardware

> *»Remember this: The math is good, but math has no agency.*
> *Code has agency, and the code has been subverted.«*
>
> *– Bruce Schneier, 5. September 2013*

Es gibt ein eigenes Teilgebiet der Kryptographie namens *Kleptographie*, welches sich unter anderem mit dem sicheren Stehlen von Geheiminformationen durch Manipulation von Software und Hardware beschäftigt. Ohne Einsicht in den Source- Code und das Hardware-Design ist der Angegriffene beweisbar hilflos.

Nach Snowden ist dollargenau bekannt, dass die Geheimdienste über einen Milliarden-Etat verfügen, um die Sicherheit von kommerzieller Software und Geräten mit Hintertüren zu versehen. Lesbarer Quellcode und aufmerksame Entwickler bieten hiergegen Sicherheit.

Lesbarer Quellcode bedeutet nicht zwangsläufig die Verwendung einer offenen Lizenz. Auch veröffentlichter Quellcode kann unter kommerzielle Lizenzen gestellt werden, die die Verwendung und Weitergabe nahezu beliebig einschränken können. Shared Code Initiativen, die beispielsweise Microsoft mit verschiedenen Regierungen vereinbart hat, bieten geringeren Schutz, da nicht die gesamte kryptographische Forschungsgemeinde an der Sicherheitsanalyse teilnehmen kann. Die freie Forschung arbeitet besser als ihre Gegenspieler im Verborgenen und tut dies in der Regel kostenlos für (akademischen) Ruhm und Ehre.

Eine einfache Empfehlung

Aus der Sicht der theoriekundigen Praktiker und der praktisch orientierten Theoretiker ergeben sich überraschend einfache Empfehlungen mit zu vernachlässigenden Kosten:

Starke Kryptographie mit extra Sicherheitsspielraum.

Dies bedeutet beispielsweise

- die Verwendung von 256-Bit Schlüssellänge für AES
- Schlüssellänge größer gleich 4096 Bit für RSA
- 512-Bit Hashfunktionen

Ohne volle Schlüsselkontrolle für die Anwender und ohne lesbaren Code und offene Hardware helfen die besten kryptographischen Verfahren natürlich nicht gegen Geheimdiensthintertüren.

Starke Kryptographie als Standardeinstellung

Anbieter von Internet-Dienstleistungen sollten verpflichtet werden, sichere Kryptographie als Standardeinstellung zu nutzen.

Die Enthüllung zum Behördenvorgehen gegen den Mail-Anbieter Lavabit zeigen, wie riskant kryptographisch problematische Einstellungen sind. Es scheint noch nicht bei allen Verantwortlichen angekommen zu sein, aber beim Benutzen der Standardeinstellungen bedeutet die erzwungene Herausgabe von TLS-Schlüsseln die automatische Kompromittierung der gesamten, sicherlich von der NSA aufgezeichneten, Kommunikation *aller* Kunden.

Der getroffene Mail-Anbieter Lavabit beendete den Geschäftsbetrieb, Kommentatoren schrieben über das »Todesurteil für US-Kryptographie« und für US-Cloudanbieter könnte dies in der Tat das Aus des Nicht-US-Geschäftes bedeuten.

Doch auch hier ist dank kryptographischer Forschung die Lösung nur einen Mausklick entfernt. Perfect Forward Secrecy (PFS) ermöglicht, dass durch eine Kompromittierung eines TLS-Serverschlüssels nicht die gesamte Kommunikation von Unschuldigen betroffen ist. Die Forschung

macht keinen Unterschied, ob die Kompromittierung der Schlüssel illegal oder formal gesetzeskonform geschehen ist.

Nach Snowden sollten RSA1024 und RC4 nicht mehr verwendet und die Schlüsselvereinbarung auf Perfect Forward Secrecy umgestellt werden.

Im Oktober 2013 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den »Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung«:

> *»Demnach wird in der Bundesverwaltung das Protokoll TLS 1.2 in Kombination mit Perfect Forward Secrecy (PFS) als Mindeststandard auf beiden Seiten der Kommunikationsbeziehung vorgegeben.«*

Diese für die Kundensicherheit notwendigen Änderungen sind durch wenige Mausklicks in der Servereinstellung zu erreichen.

Kryptographische Forschung nutzen!

Kryptographie ist eine notwendige Technologie zum Schutz des freiheitlich demokratischen Gemeinwesens. Trotz der viel diskutierten Angriffe ist es stets die schlechteste Lösung, ungeschützt zu kommunizieren. Werkzeuge wie die Browsererweiterung HTTPS Everywhere der Bürgerrechtsvereinigung EFF unterstützen sicherere Kommunikation ohne weiteres Zutun.

Die kryptographische Forschung entwickelt schon seit vielen Jahren Protokolle, die für die menschliche Gestaltung einer digitalen Gesellschaft hilfreich sein könnten.

So ermöglicht das in viele Jabber-Programme integrierte OTR-Protokoll, soziale Eigenschaften eines privaten Gespräches in der digitalen Welt nachzubilden. Fortschrittliche Kryptographie kann sogar, sich bei oberflächlicher Betrachtung ausschließende, Eigenschaften wie Zurechenbarkeit und Schutz gegen Veröffentlichung miteinander in Einklang bringen.

Auch digitales Geld und anonyme Abstimmungsverfahren können durchaus wünschenswerte Bereicherungen des Zusammenlebens mit sich bringen. Viele neue Ideen aus der Kryptographie warten auf Anwendung. Und die Zeit drängt.



Interviews

Interview mit Johannes Caspar

Prof.Dr.Johannes Caspar ist Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit sowie Rechtswissenschaftler mit besonderen Schwerpunkten im Bereich des öffentlichen Rechts und der Rechtsphilosphie

Waren Sie überrascht als sie von den ersten Enthüllungen hörten?

Dass eine erhebliche Überwachung seitens der Geheimdienste erfolgt, war natürlich zu erwarten. Sowohl qualitativ als auch quantitativ hat mich das Ausmaß dann aber doch überrascht. Vorgänge, von denen man lediglich eine eher unscharfe Vorstellung hat, kommen einem naturgemäß weniger nahe, als wenn sie unmittelbar wahrnehmbar dokumentiert werden. Es ist der große Verdienst von Edward Snowden, den Blick hierauf geschärft zu haben: Um unsere digitalen Grundrechte steht es derzeit erdenklich schlecht.

Welche Auswirkungen auf Individuum und Gesellschaft hat die enthüllte Überwachungsmaschinerie im Gesamtbild?

Die 1980er Jahre waren vom Misstrauen gegen einen datenverarbeitenden Nationalstaat geprägt. Die Volkszählung als vergleichbar harmlose Veranstaltung staatlicher Datensammelei hatte aber immerhin genug Sprengkraft, um vielen die Bedeutung des Datenschutzes vor Augen zu führen. Im weiteren Verlauf insbesondere des letzten Jahrzehnts hat sich im Zuge einer Ökonomisierung von personenbezogenen Daten als Tauschmittel einer vermeintlichen Gratiskultur im Internet dann die Entwicklung hin zur Überwachungsgesellschaft ergeben. Die nunmehr dokumentierte Internationalsierung von Überwachungsaktivitäten durch Geheimdienste markiert einen weiteren Schritt und stellt eine massive Synthese dieser Entwicklungslinien dar: Über Programme wie Tempora, XKeyscore und PRISM wird der Zugriff auf den digitalen Datenstrom in Echtzeit mit dem Zugang auf die gesammelten Nutzerdaten der Internetdienste als den Hauptakteuren der Überwachungsgesellschaft verknüpft. Dies ist der großangelegte Versuch, die digitale Infrastruktur gegen den Nutzer zu kehren und möglichst alle Daten von Informations-

und Kommunikationsprozessen unter ständige Überwachung zu bringen. Die digitale Kommunikation des Einzelnen ist seither mit dem Bewusstsein ständiger Überwachung notwendig verbunden. Statt freier Kommunikation entstehen ein permanenter Anpassungs- und Überwachungsdruck und ein diffuses Gefühl des Misstrauens. Das sind nicht die Rahmenbedingungen, die das Grundgesetz für die freie Entfaltung des Einzelnen fordert.

Müssen wir uns jetzt damit abfinden, dass die massenhafte Überwachung normal ist und sein muss, wie die Bundesregierung uns das erklären will?

Das wäre schlimm. Es wäre eine Kapitulation des Rechts- und Verfassungsstaats vor einer Sichtweise, die das technisch Machbare im vermeintlichen Kampf gegen den Terrorismus für legitim hält. Dieses kann sich auf Dauer für die Grundstruktur des Verfassungsstaats fatal auswirken. Wenn nur noch die Hoffnung der Bürger, der Staat werde im Kampf um die Sicherheit schon im Großen und Ganzen den Rahmen des rechtlich Zulässigen nicht überschreiten, uns von einem missbräuchlichen Einsatz dieser mächtigen Überwachungsinstrumente trennt, dann ist unsere Demokratie in Gefahr. Es gilt daher, Transparenz und Kontrolle gerade auch in diesem grundrechtssensiblen Bereich künftig herzustellen.

Gelten unsere Grundrechte nur auf »deutschem Boden«?

Die Diskussion, insbesondere wie sie von Vertretern der Bundesregierung geführt wurde, suggeriert dies. Doch das ist nicht richtig. Das Grundrecht des Telekommunikationsgeheimnisses wie auch das der informationellen Selbstbestimmung bindet die deutsche Staatsgewalt. Die Grundrechte gelten dann auch im exterritorialen Bereich, etwa bei der strategischen Telekommunikationsüberwachung unmittelbar durch deutsche Dienste. Sie gelten insbesondere gegenüber Ausländern, die von diesen überwacht werden, denn es handelt sich hier nicht um Rechtsgarantien, die ausschließlich deutschen Staatsbürgern zustehen. Das bedeutet in letzter Konsequenz: Auch hier sind rechtsstaatlich bestimmte Eingriffsnormen und das Verhältnismäßigkeitsprinzip unter dem Kontrollmaßstab des Art. 10 Abs. 1 GG maßgebend.

Mittlerweile ist klar, dass auch BND und Verfassungsschutz mit NSA & Co. kooperieren, indem sie Daten und Software austauschen. Gibt es dafür rechtliche Bedenken?

Die umfassende strategische Telekommunikationsüberwachung im Ausland ohne unmittelbaren territorialen Bezug und der Austausch der daraus gewonnenen Daten zwischen den Geheimdiensten sind rechtsstaatlich problematisch. Es muss künftig sicher gestellt werden, dass nicht nach dem Muster vorgegangen werden kann: »Ich überwache deine Staatsbürger und du meine, und dann tauschen wir unsere Daten«.

Brauchen wir eine effektivere Kontrolle der Geheimdienste und wenn ja, wie könnte die aussehen?

Der Rechtsstaat beruht auf dem Gedanken der demokratischen Kontrolle und Begrenzung von staatlicher Macht. Die Nachrichtendienste machen hier keine Ausnahme. In den letzten Jahrzehnten hat es technische Entwicklungen gegeben, die sich als Risikotechnologien für eine weltumspannende Überwachung der Menschen auswirken. Das Modell der demokratischen Kontrolle muss den gewaltigen Risikopotentialen der Überwachungstechnologien angepasst werden. Zunächst muss daher die alte Architektur der Regelung der deutschen Nachrichtendienste auf den Prüfstand. Es bedarf Gremien, die unabhängig, professionell und gut ausgestattet ihrer Kontrollaufgabe gerecht werden können. Ferner brauchen wir eine stärkere Kultur der Transparenz, die grundsätzlich auch vor den wesentlichen Fragen der Arbeit von Nachrichtendiensten und ihrer Kooperationsbeziehungen nicht Halt macht.

Überwachungs-Befürworter argumentieren unter anderem, dass man ein Recht auf Privatsphäre verwirkt, wenn man digitale Dienste nutzt, vor allem amerikanischer Firmen. Müssen wir zukünftig in den Wald gehen, um privat kommunizieren zu können?

Dass man seine privaten Rechte verwirkt, wenn man die großen US-Internetanbieter nutzt, würden diese wohl selbst am heftigsten dementieren. Dass diese sich gegenwärtig in einer Vertrauenskrise

befinden, aus der sie aus eigener Kraft nicht herauskommen werden, ist eine neue Erfahrung für sie. Wir können und wir wollen die technischen Entwicklungen der Kommunikation und Information nicht zurückdrehen. Wir müssen aber die Bedingungen neu verhandeln, mit denen sich Staaten über die Anbieter von Kommunikations- und Informationsdiensten beliebig die Daten der Nutzer verschaffen können.

Welche konkreten Schritte können auf nationaler und internationaler Ebene unternommen werden, um diese Überwachung zurückzudrängen?

Angesichts der Komplexität des Überwachungsproblems müssen unterschiedliche Ansätze zum Einsatz kommen. Wichtig ist zunächst die internationale Dimension. Wir brauchen völkerrechtlich verbindliche Regelungen zum Schutz der digitalen Grundrechte, gerade im Verhalten der westlichen Demokratien untereinander. Daneben ist es erforderlich, dass sich die EU mit einem einheitlichen Datenschutzrecht gegen die flächendeckende Überwachung einsetzt und auch die Charta der Grundrechte gegenüber einzelnen Mitgliedstaaten durchsetzt. Auf nationaler Ebene ist die Kontrolle der Geheimdienste zu aktivieren. Hier sollte darüber nachgedacht werden, die Datenschutzbeauftragten künftig in diese Aufgabe einzubinden. Ein weiterer Ansatzpunkt ist die öffentliche Förderung einer datensicheren Infrastruktur, die künftig eine anonyme Nutzung von Telekommunikationsangeboten ermöglicht.

Im Moment sieht es so aus, als würde das mediale und politische Interesse an der Thematik sinken. Was haben die Enthüllungen konkret gebracht?

Die Enthüllungen haben die Dimensionen der Überwachung vor Augen geführt. Es kann nun niemand mehr sagen, er hätte nichts gewusst. Wenn die öffentliche Präsenz des Themas sinkt, wäre dies verhängnisvoll und würde jenen Kräften helfen, die alles dafür tun, uns daran zu gewöhnen, dass wir doch eigentlich gut regiert werden und nichts zu befürchten haben.

Was kann jede/r konkret tun, um sich dagegen zu engagieren?

Jeder sollte sich darüber informieren, wie er mit seinen Daten in der Zeit nach Snowden sicherer umgehen kann. Wir dürfen unsere Aktivtäten jedoch nicht nur darauf ausrichten, uns vor der Überwachung möglichst

gut zu verstecken, vielmehr gilt es, die Verantwortung der Überwachung auch im politischen Prozess festzumachen und sich für eine Veränderung der gegenwärtigen Strukturen einzusetzen.

Das Interview führte Markus Beckedahl.

Interview mit Dirk Heckmann

Waren Sie überrascht, als sie von den ersten Enthüllungen hörten?

Ich war nicht wirklich überrascht, habe ich doch in früheren Publikationen (u.a. zum US PATRIOT Act und Cloud Computing) bereits auf Risiken des Zugriffs auf Server durch Geheimdienste hingewiesen.

Hat Sie das Gesamtausmaß überrascht?

Das auf jeden Fall. Insbesondere dachte ich bislang nicht, mit welcher Nonchalance (um es höflich auszudrücken) sich »befreundete« Staaten und Institutionen belauschen. Auf welcher Basis finden künftig vertrauliche Sitzungen statt?

Welche Auswirkungen auf Individuum und Gesellschaft hat die enthüllte Überwachungsmaschinerie im Gesamtbild?

Die Auswirkungen sind noch gar nicht abschließend zu erfassen. Es ist aber denkbar, dass der demokratische Rechtsstaat in eine Legitimationskrise gerät. Dies nicht nur durch intransparente Informationszugriffe von Sicherheitsbehörden, sondern auch durch eine abwiegelnde Haltung des Staates nach medialer Aufklärung.

Müssen wir uns jetzt damit abfinden, dass die massenhafte Überwachung normal ist und sein muss, wie die Bundesregierung uns das erklären will?

Natürlich nicht. Vielmehr brauchen wir eine offene, sachliche und sachverständige Diskussion um notwendige Grenzen für Informationszugriffe durch staatliche Behörden sowie deren Zusammenarbeit mit Internetdienstleistern.

Gelten unsere Grundrechte nur auf »deutschem Boden«?

An deutsche Grundrechte sind nur deutsche Behörden, und nicht etwa amerikanische Geheimdienste gebunden. Das hat aber nichts mit »deutschem Boden« zu tun. Der Anwendungsbereich des Grundgesetzes ist nämlich nicht territorial, sondern institutionell und funktional begrenzt. Das bedeutet, dass staatliche Schutzpflichten zum Schutz der

Privatsphäre deutscher Bürger unabhängig davon greifen, durch wen oder wie die Privatsphäre bedroht ist. Welche Schutzmaßnahmen konkret zu treffen sind, wenn ausländische Behörden die Privatsphäre bedrohen, bleibt zu diskutieren.

Mittlerweile ist klar, dass auch BND und Verfassungsschutz mit NSA & Co kooperieren, indem sie Daten und Software austauschen. Gibt es hier rechtliche Bedenken?

Die Rechtslage ist unklar und komplex. Hier besteht Klärungsbedarf. Eine internationale Zusammenarbeit von Geheimdiensten ist zwar erlaubt und auch sinnvoll. Allerdings bestehen Bedenken, wenn deutsche Behörden Daten nutzen, die sie selbst gar nicht erheben dürften.

Brauchen wir eine effektivere Kontrolle der Geheimdienste und wenn ja, wie könnte die aussehen?

Die Kontrolle deutscher Geheimdienste kann und sollte effektiver gestaltet werden. Unter anderem sollten IT-Sachverständige eine stärkere Rolle in den Kontrollgremien spielen, weil der politische Sachverstand von Abgeordneten zur Kontrolle komplexer IT-Prozesse nicht ausreicht. Der Gesetzgeber muss die »rote Linie« für die Geheimdienste stärker ausmalen.

Überwachungs-Befürworter argumentieren unter anderem, dass man ein Recht auf Privatsphäre verwirkt, wenn man digitale Dienste nutzt, vor allem amerikanischer Firmen. Müssen wir zukünftig in den Wald gehen, um privat kommunizieren zu können?

Nein. Zur informationellen Selbstbestimmung gehört auch das Recht, Kommunikationspartner und IT-Dienstleister selbst zu wählen. Wer dabei Sicherheitsrisiken eingeht, verwirkt seine Grundrechte nicht. Auch riskante Kommunikationsbeziehungen sind vom Staat im Rahmen des Möglichen zu schützen.

Welche konkreten Schritte können auf nationaler und internationaler Ebene unternommen werden, um diese Überwachung zurückzudrängen?

Zunächst einmal bedarf es einer breiten gesellschaftlichen und politischen Debatte über die Grenzen staatlicher Überwachung, aber auch über deren Notwendigkeit. Dann wird über eine Anpassung der aktuellen Sicherheitsgesetze zu reden sein. Mit einer so erlangten klaren Haltung ist schließlich die Diskussion auf der internationalen Bühne zu führen. Ziel muss es sein, staatliche Gefahrenvorsorge und internationale Kriminalitätsbekämpfung verhältnismäßig und transparent zu gestalten.

Im Moment sieht es so aus, als würde das mediale und politische Interesse an der Thematik sinken. Was haben die Enthüllungen konkret gebracht?

Sie haben auf jeden Fall Aufmerksamkeit erzeugt, eine notwendige Diskussion angestoßen und intransparente Überwachungsvorgänge wenigstens zum Teil aufgedeckt. Hier kann und muss weiter angesetzt werden. Darüber hinaus besteht Forschungsbedarf in Fragen rechtmäßiger Technik und technikgemäßen Rechts.

Das Interview führte Markus Beckedahl.

Interview mit Felix Stalder

Felix Stalder ist Professor für Digitale Kultur und Theorien der Vernetzung in Zürich, Vorstandsmitglied des World Information Institute in Wien und langjähriger Moderator der internationalen Mailingliste nettime. Er forscht u.a. zu Urheberrecht, Freier Kultur, Privatsphäre und Suchtechnologien.

Was hast Du Dir gedacht, als die ersten Snowden-Enthüllungen veröffentlicht wurden?

Zunächst fand ich es merkwürdig, dass die Veröffentlichungen von Hongkong aus geschahen. Ich wunderte mich, dass es keinen besseren Ort auf der Welt geben sollte als Hongkong, um kritisches Material zu veröffentlichen. Aber auch Hongkong, mit seiner spezifischen Situation von relativ freier Presse innerhalb des mächtigen chinesischen Staates war dafür ungeeignet. Dass es nun gerade das autoritäre Russland ist, dass als einziges Land bereit ist, Snowden aufzunehmen, ist deprimierend und ein Armutszeugnis erster Güte für alle Staaten, die vorgeben, die Pressefreiheit zu schützen.

Was denkst Du Dir jetzt nach vier Monaten Enthüllungen? Hat sich etwas verändert?

Nicht viel. Außer dass die gesamte Grundstimmung was digitale Kommunikation betrifft, deutlich dunkler geworden ist. Das Problem ist, dass es keinen mächtigen gesellschaftlichen Akteur gibt, der etwas dagegen unternehmen wollte. Die Politik nicht, die Wirtschaft sicher nicht, denn Überwachung ist ein riesiges Geschäft. Da zählen ein paar BürgerrechtlerInnen wie wir recht wenig.

Was bedeutet das für Gesellschaften, wenn wir nun herausfinden, dass wir allumfassend überwacht werden?

Wir können heute alle kommunizieren, wie das bis vor kurzem nur die Eliten konnten. Daraus ist viel Gutes entstanden, Freie Software, Freie Kultur und viele andere Nischen der freiwilligen, transparenten Kooperation. Aber der Preis der Explosion der Kommunikation ist, dass Macht sich auf die Ebene der Daten verschoben hat. Man könnte sagen,

die Internet-Revolution ist in ihre gegenrevolutionäre Phase getreten. Die Freiheitsgewinne der ersten Phase (ca. 1990-2005) werden wieder zurückgeholt und durch neue Kontrollstrukturen neutralisiert.

Was sind die politischen Forderungen, die aus dem größten Überwachungsskandal der Menschheitsgeschichte folgen müssen?

Was wir sehen ist eine Erosion der Grundrechte, allen voran des Rechts auf Privatsphäre. Wenn wir die USA anschauen, dann erschreckt mich dort am meisten, dass eine der wichtigsten Errungenschaften der Aufklärung, die Öffentlichkeit staatlichen Handelns, ganz besonders der Gerichte, quasi aufgehoben ist. Es ist heute möglich, auf Basis eines geheimen Gesetzes, durch ein geheimes Gericht verurteilt zu werden und dann gezwungen zu sein, darüber Stillschweigen zu waren. Das ist ein Rückfall in finsterste Zeiten des Absolutismus. Das ist eigentlich unvorstellbar.

Es gilt wieder, ganz basal, die Rechte der Bürger gegenüber dem Staat zu stärken, wobei man daran denken muss, dass »Staat« und »Wirtschaft« kein zwei getrennten Akteure sind, sondern wie wir auch durch Snowden erfahren haben, eng verschränkt sind. Insofern müsste man vielleicht sagen, dass die Rechte des Einzelnen gegenüber großen Institutionen gestärkt werden müssten.

Welche technischen Implikationen hat das Ganze, wenn das derzeitige Internet zu einer globalen Überwachungsinfrastruktur umgebaut wurde?

Die USA werden wohl in ihrer zentralen Position innerhalb des Netzwerkes geschwächt werden. Das Netz wird in seiner Tiefenstruktur dezentraler werden. Es werden in Zukunft wohl weniger Daten durch die USA fließen als bisher. Die Regierung von Brasilien hat bereits angekündigt, hier aktiv zu werden, und auch jede andere Regierung wird sich wohl genauer anschauen, wie ihre Daten von Punkt A nach B kommen. Das muss nicht unbedingt eine gute Sache sein, denn jede Regierung hat einen Geheimdienst, der gerne mithören würde.

Was müssen wir tun, um Menschenrechte und ein offenes Netz zu schützen?

Was von Menschen gemacht wird, kann von Menschen auch wieder verändert werden. Ein Großteil dessen, was jetzt gemacht werden muss, findet weniger auf der politisch-juristischen Ebene statt, sondern auf der politisch-technischen. Damit meine ich, dass wir uns wieder mit der Architektur der Infrastruktur und ihren politischen Dimensionen beschäftigen müssen. Als Grundsatz könnte hier gelten, Daten, die zentral anfallen, müssen offen gelegt werden. Die Open Data Bewegung macht hier wichtige Arbeit, steht aber noch sehr am Anfang. Im Gegenzug müssen Daten, die nicht öffentlich sein dürfen, wieder stärker dezentral werden. Dass wir alle unsere persönlichen Daten bei Google, Facebook und GMX lagern, ist ja eine Einladung zur Überwachung. Auch hier gibt es interessante Projekte, etwa Mailpile, um Webmail dezentralisieren zu können. Der alte CCC-Slogan »öffentliche Daten nützen, private Daten schützen« ist immer noch sehr aktuell.

Konkret zu Österreich: Gibt es bei euch eine mediale und politische Debatte zum Thema? Und wenn ja, wie verläuft die?

Ja, die gibt es, aber die komödienhaften Aspekte überwiegen. So haben etwa die Grünen gefordert, Snowden sollte Asyl gegeben werden, was aber ein reiner Wahlkampf-Gag war und nicht ernsthaft verfolgt wurde. Der Höhepunkt der Komik war die Episode, als bekannt wurde, dass sich in Wien eine NSA Lauschstation befindet. Die Politik reagierte darauf, dass sich das Verteidungsministerium, das Innenministerium und das Justizministerium für »nicht zuständig« erklärten und der Kanzler schwieg. Das hat er von Frau Merkel gut gelernt.

Das Interview führte Markus Beckedahl.

Interview mit Ot van Daalen

Ot van Daalen war bis zum 1. Oktober 2013 Direktor von Bits of Freedom, einer niederländischen Organisation für digitale Rechte.

Auf welche Weise berichteten die nationalen Medien über Snowdens Enthüllungen der massenhaften Überwachung?

In Bezug auf Snowdens Enthüllungen begannen die niederländischen Medien darauf aufmerksam zu werden, als PRISM aufgedeckt wurde. Die nationalen Fernseh-Nachrichten berichteten über das Thema zu Beginn zweimal in Folge. Seitdem flachte die Aufmerksamkeit allmählich ab.

Welche Überwachungssysteme oder -kooperationen wurden in Ihrem Land aufgedeckt?

Direkt nach PRISM wurde behauptet, der niederländische Geheimdienst überwache alle Mobilfunk-Gespräche, aber dafür gab es nicht viele Beweise. Dennoch bekommt der niederländische Geheimdienst Informationen von US-Einrichtungen und fragt nicht, woher diese stammen. Deshalb kann er Verbindungen dieser Informationen, beispielsweise zu PRISM, verschleiern.

Gab es eine Diskussion über die Enthüllungen in der Bevölkerung?
Wie groß war diese und wie war sie gestaltet?

Es gab und gibt immer noch eine Diskussion über die Enthüllungen, doch nur sehr beschränkt. Manchmal kommt etwas in Zusammenhang mit konkreten Neuigkeiten auf, aber eine breite Debatte über das Ausspionieren existiert nicht. Ein immer wiederkehrendes Thema ist, dass die Überwachungen eine Ausprägung des US-Imperialismus sind, wobei EU und die Niederlande zu stark in die Überwachungsmaschinerie involviert sind, um ernsthaft dagegen vorzugehen.

Wie reagierte die Innenpolitik auf die Überwachungsenthüllungen?
Gab es irgendwelche Veränderungen?

Die Parlamentarier erwähnen sie nicht besonders häufig, bloß in Zusammenhang mit aktueller Berichtserstattung. Im Parlament wurde eine Plenarsitzung zu dem Thema vor zwei Monaten angesetzt, dann aber verschoben und bis heute nicht wieder auf die Agenda gesetzt. Antworten der Regierung auf Anfragen von Parlamentsmitgliedern sind recht neutral und verurteilen die NSA nicht. Es gab in Politikerkreisen keinen ernsthaften Aufschrei und keine der größeren Parteien ruft zu Veränderungen der derzeitigen Situation auf. Hauptsächlich verweisen sie darauf, dass die EU die richtige Plattform ist, um sich um diese Angelegenheiten zu kümmern.

Was erzählten ihre Landesvertreter den Regierungen der »Five Eyes«-Staaten über ihre Abhörmöglichkeiten?

Das wissen wir nicht.

Was bedeutet all das für Aktivisten und Journalisten Ihres Landes?

Wir empfehlen nun Journalisten, ihre eigenen Operationen besser zu sichern (OPSEC) und der Sicherheit des Internets und von Digitaltechnologien mit grundlegendem Misstrauen zu begegnen. Aber das macht Journalisten und auch Aktivisten ihre Arbeit sehr viel schwerer.

Gibt es in Ihrem Land Proteste gegen Überwachung?

Nein.

Wie bringt sich Bits of Freedom in die Diskussion ein?

Davon abgesehen, dass wir das Ausspionieren verurteilen und die Regierung auffordern, sich ausdrücklich von der NSA zu distanzieren, nutzen wir die Enthüllungen, um die Aufmerksamkeit auf Entwicklungen in den Niederlanden zu lenken, die bereits vor den Leaks begonnen haben. Vor allem machen wir auf einen Vorschlag aufmerksam, den niederländischen Geheimdiensten mehr Überwachungsmöglichkeiten für das massenhafte Abhören von Internetverkehr zu geben.

Was sollte auf internationaler und EU-Ebene verändert werden um die Massenüberwachung im Netz zu stoppen und die Menschenrechte zu schützen?

Die EU und ihre Mitgliedsstaaten sollten Stellung beziehen und verlangen, dass die USA aufhören, normale Bürger und nicht nur Verdächtige zu überwachen. Sie sollten außerdem selbst mit dem generalisierten Ausspionieren aufhören. Transparenz und Beaufsichtigung auf beiden Seiten des Ozeans sollten unter Einsatz beträchtlicher Ressourcen merklich erhöht werden.

Das Interview führte Markus Beckedahl und wurde von der Redaktion ins Deutsche übersetzt.

Interview mit Rikke Frank Jørgensen

Rikke Frank Jørgensen ist Beraterin des Dänischen Instituts für Menschenrechte und externe Dozentin des »International Master on Communication and Globalisation« an der Roskilde Universität in Dänemark. Außerdem ist sie Expertin für die Arbeitsgruppe »Rechte der Internet Nutzer« des Europarats.

Auf welche Art berichteten die Medien in Ihrem Land über die Enthüllungen von Edward Snowden zur Massenüberwachung?

Generell war das Presse-Echo nicht besonders groß. Eine Zeitung berichtete über mehrere Wochen hinweg recht umfangreich und kritisch. Eine andere veröffentlichte eine Artikel-Reihe zum Thema »Bedrohungen des Rechts auf Privatsphäre«.

Welche Überwachungssysteme oder -kooperationen wurden in Ihrem Land aufgedeckt?

Dänemark wurde in den Enthüllungen nicht explizit erwähnt. Dennoch sind die Dänen von der Datensammlung mit Hilfe von Infrastruktur (Glasfaser-Kabel) und Diensten (z.B. Facebook) betroffen, da sie intensiv alle großen US-Dienste (Facebook, Google, Skype, Youtube, Yahoo, etc.) und die US-Internetinfrastruktur nutzen.

Gab es eine Diskussion über die Enthüllungen in der Bevölkerung?
Wie groß war diese und wie war sie gestaltet?

Es fand eine öffentliche Diskussion statt, der zufolge gab es kein großes öffentliches Bewusstsein oder Bedenken. Einige öffentliche Kommentatoren, zivilgesellschaftliche Organisationen und Politiker waren sehr kritisch. Sie haben vollen Einblick in das Ausmaß und die rechtliche Grundlage des Vorgehens der USA gefordert. Es kamen auch im Parlament Fragen über diese Angelegenheiten auf. Speziell die Aussage, dass auch europäische Politiker Gegenstand der Überwachung waren, provozierte viele Politiker.

Im Gegensatz dazu äußerte der dänische Premierminister: »Auf lange Sicht sollten die Dänen sich gut fühlen, was die US-Überwachung

anbelangt, denn sie hilft, Dänemark gegen Terrorismus zu schützen.«

Wie reagierte die Innenpolitik auf die Überwachungsenthüllungen? Gab es irgendwelche Veränderungen?

Bisher gab es keine Veränderungen in der Innenpolitik. Die Regierung und viele Kommentatoren betonen, dass es schwierig ist, zu handeln bevor wir vollen Einblick und Beweise für die Anschuldigungen haben.

Was erzählten ihre Landesvertreter den Regierungen der »Five Eyes«-Staaten über ihre Abhörmöglichkeiten?

Der dänische Premierminister traf sich kurz nach den Enthüllungen mit US-Präsident Obama. Aber außer einer allgemeinen Anerkennung ihres Gesprächs und den Erklärungen von Präsident Obama gab es wenig öffentliche Informationen über den Austausch.

Was bedeutet all das für Aktivisten und Journalisten Ihres Landes?

Im Moment scheinen die Menschen nicht sonderlich besorgt. Doch auf dem nationalen Internet Governance Forum am 26. September fand eine Versammlung von ungefähr 60 Teilnehmern statt, die sich mit diesen Themen befassten. Verschiedene Gegenmaßnahmen wurden debattiert, zum Beispiel digitale Selbstverteidigung, die Entwicklung und Förderung eines europäischen Internet Services (»NSA-freie Dienste«), die Ausübung von Druck auf EU-Politiker für ein globales Datenschutz-Abkommen usw.

Gibt es in Ihrem Land Proteste gegen Überwachung?

Nur wenige. Es gab Proteste gegen ACTA und einige in Zusammenhang mit Vorratsdatenspeicherungen, aber im Allgemeinen nicht.

Grundsätzlich ist es schwierig, Dänen gegen Überwachung zu mobilisieren. Die Menschen vertrauen der Regierung zum Großteil und sagen oftmals, dass Datensammlung ihnen persönlich nicht schaden wird. Nur wenige zivilgesellschaftliche Organisationen und Kommentatoren versuchen, eine Grundsatzdebatte zum Recht auf Privatsphäre als Fundament einer freien und offenen Gesellschaft auszulösen.

Was sollte auf internationaler Ebene verändert werden um Massenüberwachung im Internet zu stoppen und die Menschenrechte zu schützen?

Es bestehen viele Herausforderungen, aber die zwei Hauptpunkte scheinen zu sein: 1. eingeschränkte Rechtsmittel, wenn Menschenrechtsverletzungen außerhalb der eigenen Gerichtsbarkeit stattfinden und 2. Firmen, die nicht für Menschenrechtsverletzungen haftbar gemacht werden können.

Bezüglich der ersten Herausforderung kann man auf verschiedenen Wegen vorgehen. Einer könnte globales Engagement für Privatsphäre und Datenschutzstandards vorantreiben, so wie sie in »Internationale Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung« gefordert sind. Diese Grundsätze basieren auf den Menschenrechten und beleuchten die Verpflichtungen von Staaten, diese im Zusammenhang mit Kommunikationstechnologie und Überwachungsmöglichkeiten umzusetzen. Sie wurden am 20. September auf der 24. Sitzung des UN-Menschenrechtsrat eingeführt und von über 250 Organisationen unterzeichnet.

Selbst wenn Staaten sich diesen Standards verpflichten würden (was in naher Zukunft nicht sehr wahrscheinlich ist), wäre es dennoch nötig, praktische Rechtsmittel einzuführen, damit ein Bürger des Staates X wirksamen Rechtsbehelf hat, wenn in Land Y ein Verstoß stattfand.

Man kann auch die Überprüfung und Durchsetzung der existierenden Menschenrechtsstandards stärken, in diesem Fall ist das Artikel 17 (Recht auf Privatsphäre) und der internationale Pakt über bürgerliche und politische Rechte.

Eine andere Maßnahme könnte der Anstoß eines globalen Abkommens zum Datenschutz sein. Davon abgesehen, dass es noch keine politische Unterstützung zur Durchsetzung dieses Vorhabens gab, würde es auch der Durchsetzung gegenüber privaten Firmen nicht gerecht werden, es sei denn, diese wären auch Gegenstand des Abkommens.

In Zusammenhang mit der zweiten Herausforderung haben die UN-Leitprinzipien für Wirtschaft und Menschenrechte, die sogenannten

Ruggie-Prinzipien von 2011, einen globalen Standard für die Verantwortung von Unternehmen für Menschenrechte gesetzt. Initiativen wie die Global Network Initiative und Industry Dialog (ins Leben gerufen von Nordic Telecoms) sprechen sich für das Bewusstsein von Firmen über Menschenrechte aus. Das beinhaltet beispielsweise den Aufruf für die Sorgfaltspflicht bezüglich der Identifikation, Vorbeugung, Abmilderung, und Verantwortlichkeit, wenn Unternehmen Menschenrechte verletzen. Das beinhaltet auch Prozesse, um Schwächungen von Menschenrechten zu beseitigen, zu denen die Firmen beitragen.

Diese Grundprinzipien wurden von den EU-Richtlinien fortgesetzt, die insbesondere den IT-Sektor adressieren.

Trotz des wachsenden Bewusstseins der Verantwortung gegenüber Menschenrechten in der Privatwirtschaft und den verschiedenen Industrie-Initiativen, um die Befolgung der Prinzipien sicherzustellen, basieren sie immer noch auf Freiwilligkeit, ohne die rechtliche Möglichkeit einer Durchsetzung.

Da der Staat die Pflicht hat, seine Bürger gegen Menschenrechtsverletzungen zu schützen, was private Unternehmen einschließt, wäre es ein einfacher Schritt vorwärts, Privacy- und Datenschutzstandards in nationales Recht zu überführen, das bindend für Unternehmen ist. Ein starkes US-Datenschutzgesetz würde die Spielregeln für viele der großen Internetfirmen verändern. Dennoch, das würde weder das Problem des Rechtsanspruchs von Nicht-US-Bürgern lösen noch ist es wahrscheinlich, dass so etwas in naher Zukunft passieren wird.

Das Interview führte Markus Beckedahl und wurde von der Redaktion ins Deutsche übersetzt.

Interview mit Renata Avila Pinto

Renata Avila Pinto ist Anwältin für Urheberrecht. Sie ist bei Creative Commons Guatemala als Projektleiterin tätig. Momentan arbeitet sie an Fällen zu internationalen Menschenrechten und als unabhängige Forscherin an Themen der Privatsphäre, Zugang zu Wissen und Redefreiheit für das Cyberstewards Netword, Citizen Lab, Universität Toronto.

Als die ersten Snowden-Leaks veröffentlicht wurden: Was dachten Sie?

Solange die Quelle noch anonym war, habe ich mir ernsthafte Sorgen über seine/ihre körperliche Unversehrtheit gemacht. Mir ist klar geworden, dass die Enthüllungen eine direkte Bedrohung für den Status Quo der verstärkt miteinander verflochtenen Allianz mächtiger, multinationaler Technologiekonzerne mit den mächtigsten Staatsregierungen der Welt darstellen. Es hat mich zum Nachdenken darüber gebracht, dass es an Mechanismen für den Schutz journalistischer Quellen mangelt und wir ein Unterstützungsnetzwerk für sie brauchen. Eine Informationsquelle ist meiner Meinung nach genauso wichtig wie die Enthüllungen selbst.

Auf welche Weise berichteten die nationalen Medien über Snowdens Enthüllungen der massenhaften Überwachung?

Es wurde nur das berichtet, was von AP oder anderen Presseagenturen kam. Es gab keine gezielte Berichterstattung über die enthüllten Problematiken, nicht einmal als die XKeyscore-Karte zeigte, dass ganz Zentralamerika Knotenpunkt verschiedener Spähzentren war.

Gab es eine Diskussion über die Enthüllungen in der Bevölkerung?
Wie groß war diese und wie war sie gestaltet?

Es war eine schlecht informierte, eingeschränkte Debatte unter Eliten und Meinungsführern, von denen ein Großteil sich des gesetzlichen Rahmens nicht bewusst war, der die Privatsphäre von Bürgern länderübergreifend schützt. Jeder hat die Doppelmoral hervorgehoben: Die Verteidigung von Menschenrechten auf der einen Seite und die Art,

wie ein mächtiger Staat im Geheimen operiert, auf der anderen. Aber in einem Land mit einer langen, komplexen Historie von Überwachung, in dem ein Terrorstaat über drei Jahrzehnte gegen die eigenen Bürger gearbeitet hat, kamen die Enthüllungen nicht überraschend. Es gab einige Versuche, herauszufinden, welche Gerätschaften die lokalen und regionalen Geheimdienste benutzen, aber das hat kaum an der Oberfläche des Problems gekratzt.

Unterscheidet sich die Diskussion in Guatemala von der in anderen süd- und mittelamerikanischen Ländern?

Es gibt mehrere Parallelwelten in Lateinamerika, man könnte den Kontinent praktisch in zwei oder sogar drei Gruppen aufteilen. Auf der einen Seite gibt es die Länder, die nach den bewaffneten Konflikten eine zwar nicht perfekte, aber doch positive Wandlung vollzogen haben: Chile, Argentinien, Uruguay und zu gewissen Teilen Brasilien, wo Teile der Bevölkerung, zumindest die organisierte Zivilgesellschaft, sich der Gefahren eines Polizeistaates bewusst sind, wo es Rechenschaftspflichten und Justiz gibt und wo die Bevölkerung im Allgemeinen ihre Rechte versteht und durchsetzt. Obwohl manche der Staaten korrupt sind, sind sie dennoch stabil und die Bürger können ihre Rechte einfordern und durchsetzen.

Leider gehört Guatemala nicht dazu. Guatemala ist Teil des nördlichen Dreiecks, dem gefährlichsten Gebiet in der Region, wo Drogenkriminalität so viele Menschen tötet wie in ganz Syrien getötet wurden. Mexiko, Guatemala, El Salvador und Honduras leiden unter einem ständigen gewalttätigen und bewaffneten Konflikt, der mit dem Drogenkrieg in enger Verbindung steht. Tausende verschwundener Menschen, eine ärmliche und instabile Strafverfolgung und ein starker Einfluss der US-Sicherheitspolitik – das ist das Szenario des »Kriegs gegen Drogen«. Und wie in jedem Krieg gegen ein »Nomen« – Krieg gegen Drogen, Krieg gegen Terrorismus, etc. – verschwimmen Grenzen und Ausnahmen werden zur Regel. Die Sonderstellung all der Gesetze, die in der Region zum Kampf gegen Drogen erlassen wurden, haben zu einer Erosion der Grundrechte geführt, unter ihnen auch das Recht auf Privatsphäre. Überwachung, CCTV-Kameras, mobile Registrierung,

biometrische Pässe und verstärkte staatliche Kontrollen werden von der Zivilbevölkerung freudig begrüßt. In diesen pervertierten Cocktail mischt sich dann noch die enge, außerrechtliche Zusammenarbeit von Telekommunikationsunternehmen mit den Strafverfolgungsbehörden. Überwachung ohne vorherigen richterlichen Beschluss wurde sogar von der internationalen Kommission zur Bekämpfung der Straflosigkeit in Guatemala (CICIG) vorangetrieben. Sie haben nicht nur eine Verordnung vorgeschlagen, die der Polizei erlaubt, digitale Überwachung ohne Anordnung durchzuführen, sondern auch Ausrüstung dafür finanziert.

Was haben Ihre Regierungsvertreter den »Five Eyes«-Staaten zu deren Abhörkapazitäten gesagt?

Eine sehr schwache Gruppe von Mitgliedern des Kongresses hat das Ganze in begrenztem Rahmen hinterfragt. Aber da Guatemala in keinem Dokument ausdrücklich erwähnt wird und lokale Journalisten keinen Zugang zu den Dokumenten haben, gibt es auch noch keine Diskussion. Die Regierung und die Ausrüstung, Ausbildung und Finanzierung der Polizei sind stark abhängig vom Geld der »Five Eyes«-Staaten. Sie werden diese Finanzierung nicht durch Kritik aufs Spiel setzen. Ich frage mich, ob sie Zugang zu den Geheimdienstinformationen von NSA und dem wichtigsten Akteur in dieser Gegend, DEA, haben.

Wo liegt das Problem mit dem allgegenwärtigen Überwachungsstaat, dem wir uns gegenübersehen und der versucht, jede digitale Kommunikation auf der Erde abzufangen?

Durch totale Überwachung und totale Kontrolle wird kein Widerspruch mehr möglich sein. Ich bin sehr beunruhigt über das Risiko einer totalitären globalen Gesellschaft, in der Grundrechte effektiv unterdrückt werden, um die Rechte Weniger zu schützen. Ich bin auch sehr besorgt, da Ausrüsten und Entwerfen der Überwachungstechnologien, -mechanismen und -werkzeuge Teil der zwei größten Sektoren sind: dem Technik- und dem Sicherheitssektor, sehr zentrale Industriezweige für die Länder der Ersten Welt. Vorrangig für die »Five Eyes« und europäische Länder. Selbst wenn alle lateinamerikanischen Bürger ihre Stimme erheben würden, könnten sie ein solches Modell nicht umkehren und abschaffen.

Das Traurige daran ist, dass unsere Staaten aus der jüngsten Vergangenheit noch den Missbrauch kennen, den ein Staat begeht, wenn er absolute Kontrolle über die Daten, Bewegungen, Ideen und Interessen eines Bürgers hat – vor allem wenn dieser Bürger den Mächtigen nicht zustimmt.

Die Aktivitäten der Industrie, die am schwersten zur Rechenschaft gezogen werden kann, und der undurchsichtigsten Institution, den Geheimdienstbehörden, sind unter dem Segel der nationalen Sicherheit geschützt. Sie nehmen Bürgern und Parlamentariern die Möglichkeit, mitzubekommen, was passiert. Wenn man darüber nachdenkt, können diese beiden Gruppen sogar mächtiger sein als der Präsident eines Landes.

Was bedeutet all das für Aktivisten und Journalisten Ihres Landes?

Unsichere Kommunikation und unsichere Geräte, die dafür entworfen wurden, abgehört zu werden, stellen für jeden ein Risiko dar. Der Mangel an Transparenz nimmt uns die Möglichkeit, zu wissen a) zu welchen Technologien unsere außerordentlich korrupte Regierung Zugang hat, b) ob NSA und DEA Geheimdienstinformationen mit unserer Regierung austauschen. Außerdem besteht die Möglichkeit, dass Drogenkartelle Zugriff auf solche Informationen bekommen, denn es ist bekannt, dass viele der Institutionen von der Narco infiltriert sind. Deshalb sind die NSA-Enthüllungen schlechte Neuigkeiten für beide Gruppen, vor allem die Journalisten, die über den Drogenkrieg berichten und jene Journalisten und Aktivisten, die sich gegen den Bergbau durch kanadische und amerikanische Firmen aussprechen. Die Enthüllungen über das illegale Ausspionieren des brasilianischen Energieministers hat meine Sorge um Anti-Bergbau-Aktivisten noch verstärkt.

Gibt es in Ihrem Land Proteste gegen Überwachung?

Nein, tatsächlich hat die Zivilgesellschaft gerade erst eine Kampagne gestartet und ein Gesetz zur Stärkung der Kontrolle und Überwachung von Mobilfunk erwirkt.

Was müssen wir tun, um Menschenrechte und ein offenes Internet zu schützen?

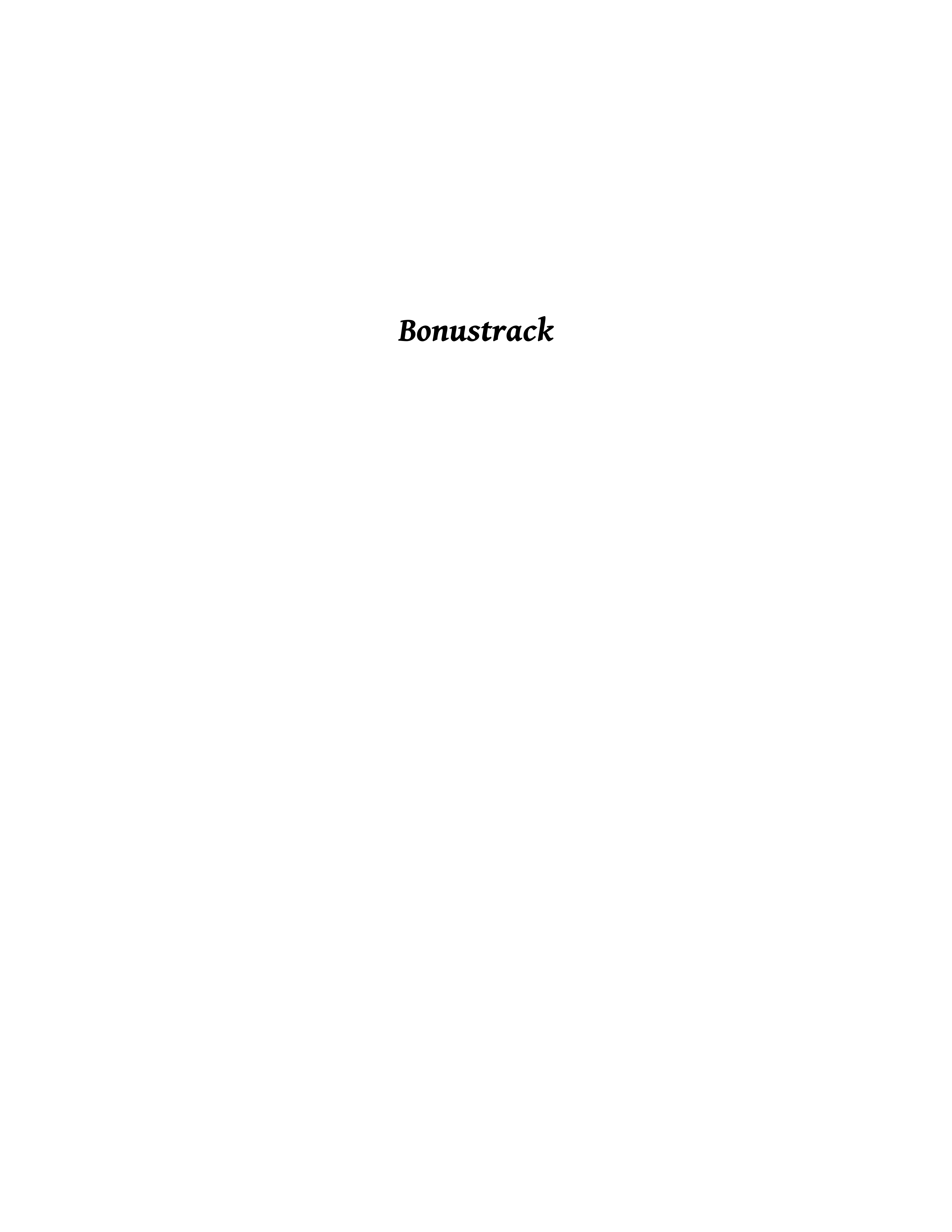
Es ist dringend notwendig, einen globalen Rechtekatalog für Internetnutzer voranzutreiben. Der durchschnittliche Nutzer muss seine Rechte und Freiheiten kennen und wissen, was Regierungen – manchmal auch fremde Regierungen – tun, um die Ausübung dieser Rechte einzuschränken.

Es gibt also keinen echten politischen Umschwung?
Woran liegt das? Und wie können wir das ändern?

Es gibt die sehr schädliche Annahme, dass das NSA-Problem durch den US-Kongress gelöst werden wird. Aber tatsächlich wird das globale Überwachungsproblem sowohl lokal als auch global gelöst werden.

Auf lokaler Ebene müssen wir verlangen, über das Ausmaß und die Begrenzungen der Inlandsüberwachung Bescheid zu wissen und bessere Standards dafür fordern. Außerdem müssen unsere Autoritäten unser Recht auf Privatsphäre verteidigen. Ein Staat kann einige Zielpersonen mit richterlichen Anordnungen und angemessenen Schutzvorkehrungen überwachen. Ein Land darf es einem anderen nicht erlauben, seine Einwohner auszuspähen. Ein fremdes Land hat kein Recht dazu. Das ist die starke Forderung auf globaler Ebene, eine Forderung, die voraussetzt, dass mächtige Branchen, deren Kerngeschäft durch Ausspähung unterwandert ist, ihren Einfluss geltend machen und die Achtung der Gesetze fordern. Das ist eine Angelegenheit der nationalen Sicherheit, des Handels, der Souveränität und Ehre. Es geht darum, Recht zu respektieren, das Recht von allen, universelle Rechte.

Das Interview führte Markus Beckedahl und wurde von der Redaktion ins Deutsche übersetzt.



Bonustrack

Petitionstext von stopsurveillance.org

Wir, die nachfolgenden Unterzeichnerinnen und Unterzeichner, fordern unsere Regierung, unser nationales Parlament, die EU-Kommission, den Europäischen Rat und das Europäische Parlament auf:

1. Sich gegen jede Form anlassloser und unverhältnismäßiger Überwachungsmaßnahmen auszusprechen und danach zu handeln.
2. Das Recht auf Privatsphäre und Informationelle Selbstbestimmung zu achten und dieses sowohl auf nationaler Ebene wie auch in der EU-Datenschutz-Grundverordnung als auch der Datenschutzrichtlinie und den entsprechenden Normen für EU-Institutionen zu verankern und an erste Stelle zu rücken.
3. In internationalen Verträgen den Schutz und die Achtung der Privatheit und entsprechende Rechtsmittel auch gegen Überwachungsmaßnahmen durch Drittstaaten zu erwirken.
4. Zu gewährleisten, dass personenbezogene Daten, die in der EU verarbeitet werden, nicht ohne Rechtshilfeabkommen und ausreichenden Rechtsschutz an Behörden oder Organisationen in Drittländern übermittelt werden.
5. Das Grundrecht auf Gewährleistung der Vertraulichkeit und die Integrität informationstechnischer Systeme sicherzustellen.
6. Internationale Kooperationen zwischen Strafverfolgungsbehörden, Justiz und Geheimdiensten nicht zur Umgehung innerstaatlichen Grundrechtsschutzes zu missbrauchen.
7. Alle Verträge, Gesetze und Maßnahmen, die die Informationelle Selbstbestimmung der Bürgerinnen und Bürger des jeweils eigenen Landes und der EU betreffen, unmittelbar offenzulegen.
8. Die Verletzung der Privatsphäre ihrer jeweiligen Bürgerinnen und Bürger durch Unternehmen, Drittstaaten oder dort ansässige Unternehmen rechtlich, wirtschaftlich und politisch zu sanktionieren.
9. Eine individuelle Benachrichtigungspflicht der betroffenen Bürgerinnen und Bürger innerhalb möglichst kurzer Frist nach Durchführung jeder digitalen Einsichtnahme und

Überwachungsmaßnahme einzuführen, ob durch Strafverfolgungsbehörden oder Geheimdienste.

10. Projekte und Technologien zum informationellen Selbstschutz und freie und quelloffene Umsetzungen aktiv zu fördern und selbst verpflichtend zu nutzen.
11. Staatliche Überwachungspraktiken, die ohne rechtlichen Rahmen stattfinden, umgehend abzustellen.
12. Whistleblowern, die gesellschaftlich relevante Missstände aufzeigen, angemessenen rechtlichen Schutz zu garantieren.

Internationale Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung

necessaryandproportionate.org[274]

Während die Technologien, welche die staatliche Kommunikationsüberwachung unterstützen, verbessert werden, vernachlässigen die Staaten, sicherzustellen, dass Gesetze und Verordnungen in Bezug auf Kommunikationsüberwachung in Einklang mit internationalen Menschenrechten stehen und die Rechte auf Privatsphäre und Meinungsfreiheit beachtet werden. Dieses Dokument versucht zu erklären, wie internationale Menschenrechte in der aktuellen digitalen Umgebung anwendbar sind, besonders vor dem Hintergrund des Wachstums und des Wandels der Technologien und Methoden der Kommunikationsüberwachung. Diese Grundsätze können zivilgesellschaftlichen Gruppen, der Wirtschaft, Staaten und anderen einen Rahmen liefern, mit dem sie bewerten können, ob aktuelle oder geplante Überwachungsgesetze oder -praktiken im Einklang mit den Menschenrechten stehen.

Diese Grundsätze sind das Ergebnis einer globalen Beratung von Gruppen der Zivilgesellschaft, der Wirtschaft und internationalen Experten für Recht, Politik und Technologien in der Kommunikationsüberwachung.

Einleitung

Privatsphäre ist ein Grundrecht, das wesentlich für den Erhalt von demokratischen Gesellschaften ist. Es ist Voraussetzung für die menschliche Würde und verstärkt andere Rechte, wie Meinungs-, Informations- und Versammlungsfreiheit, und es ist nach internationalen Menschenrechtsgesetzen anerkannt[275]. Aktivitäten, die das Recht auf Privatsphäre begrenzen, einschließlich Kommunikationsüberwachung, können nur dann als gerechtfertigt gelten, wenn sie gesetzlich vorgeschrieben sind, sie notwendig sind, um ein legitimes Ziel zu erreichen, und sie dem Ziel, welches sie verfolgen,

angemessen sind[276]. Vor der öffentlichen Einführung des Internets schufen fest etablierte legale Grundsätze und der Kommunikationsüberwachung innewohnende logistische Hürden Grenzen für die staatliche Kommunikationsüberwachung. In gegenwärtigen Dekaden haben die logistischen Barrieren der Überwachung abgenommen und die Anwendung der gesetzlichen Grundsätze in neuen technologischen Kontexten ist unklarer geworden. Die Explosion der Inhalte digitaler Kommunikation und Information über Kommunikation, sogenannte »Verbindungsdaten« – Informationen über die Kommunikation eines Individuums oder die Nutzung elektronischer Geräte –, die sinkenden Kosten der Speicherung und des Dataminings und die Bereitstellung von persönlichen Inhalten durch Drittanbieter machen staatliche Überwachung in einem beispiellosen Ausmaß möglich[277]. Dabei haben Konzeptualisierungen der bestehenden Menschenrechtsgesetze nicht Schritt gehalten mit den modernen und sich verändernden Möglichkeiten der Kommunikationsüberwachung des Staates, der Fähigkeit des Staates, aus verschiedenen Überwachungstechniken gewonnene Informationen zu kombinieren und zu organisieren, oder der erhöhten Sensibilität der Informationen, die zugänglich werden. Die Häufigkeit, mit der Staaten Zugang zu Kommunikationsinhalten und -metadaten suchen, steigt dramatisch – ohne angemessene Kontrolle[278]. Wenn Kommunikationsmetadaten aufgerufen und analysiert werden, kann damit ein Profil einer Person, einschließlich des Gesundheitszustandes, politischer und religiöser Ansichten, Verbindungen, Interaktionen und Interessen, erstellt werden. So werden genauso viele oder sogar noch mehr Details offengelegt, als aus dem Inhalt der Kommunikation erkennbar wäre[279]. Trotz des riesigen Potenzials für das Eindringen in das Leben eines Menschen und der abschreckenden Wirkung auf politische und andere Vereinigungen, weisen rechtliche und politische Instrumente oft ein niedrigeres Schutzniveau für Kommunikationsmetadaten auf und führen keine ausreichenden Beschränkungen dafür ein, wie sie später von Behörden verwendet

werden, einschließlich wie sie gewonnen, geteilt und gespeichert werden.

Damit Staaten tatsächlich ihren internationalen menschenrechtlichen Verpflichtungen in Bezug auf Kommunikationsüberwachung nachkommen, müssen sie den im Folgenden genannten Grundsätzen entsprechen. Diese Grundsätze gelten für die Überwachung der eigenen Bürger eines Staates, die in seinem eigenen Hoheitsgebiet ausgeführt wird, sowie der Überwachung anderer in anderen Gebieten. Die Grundsätze gelten außerdem unabhängig vom Zweck der Überwachung – Strafverfolgung, nationale Sicherheit oder sonstige behördliche Ziele. Zudem gelten sie sowohl für die Aufgabe des Staates, die Rechte des Einzelnen zu respektieren und zu erfüllen, als auch für die Verpflichtung, die Rechte des Einzelnen vor Missbrauch durch nicht-staatliche Akteure, einschließlich der Wirtschaft, zu schützen[280]. Der private Sektor trägt die gleiche Verantwortung für die Wahrung der Menschenrechte, insbesondere in Anbetracht der Schlüsselrolle, die er bei der Konzeption, Entwicklung und Verbreitung von Technologien spielt und damit Kommunikation ermöglicht und bereitstellt und – wo erforderlich – staatlichen Überwachungsmaßnahmen zuarbeitet. Dennoch ist der Umfang der vorliegenden Grundsätze auf die Pflichten des Staates beschränkt.

Veränderte Technologie und Definitionen

»Kommunikationsüberwachung« umfasst heutzutage Überwachung, Abhören, Sammlung, Analyse, Nutzung, Konservierung und Aufbewahrung von, Eingriff in oder Zugang zu Informationen, welche die Kommunikation einer Person in der Vergangenheit, Gegenwart oder Zukunft beinhalten, reflektieren oder sich daraus ergeben. »Kommunikation« beinhaltet Aktivitäten, Interaktionen und Transaktionen, die über elektronische Medien übertragen werden, wie z. B. Inhalt der Kommunikation, die Identität der an der Kommunikation Beteiligten, Standort-Tracking einschließlich IP-Adressen, Uhrzeit und Dauer der Kommunikation und Kennungen von

Kommunikationsgeräten, die während der Kommunikation verwendet werden.

Traditionell wurde die Invasivität der Kommunikationsüberwachung auf Basis von künstlichen und formalen Kategorien bewertet. Bestehende rechtliche Rahmenbedingungen unterscheiden zwischen »Inhalt« oder »Nicht-Inhalt«, »Teilnehmerinformation« oder »Metadaten«, gespeicherten Daten oder Übertragungsdaten, Daten, die zu Hause gespeichert werden oder die im Besitz eines dritten Dienstanbieters sind[281]. Allerdings sind diese Unterscheidungen nicht mehr geeignet, den Grad des Eindringens von Kommunikationsüberwachung in das Privatleben von Einzelpersonen und Verbänden zu messen. Während seit langem Einigkeit darüber besteht, dass Kommunikationsinhalte per Gesetz signifikanten Schutz verdienen, da sie sensible Informationen offenbaren können, ist nun klar, dass andere Informationen aus der Kommunikation – Metadaten und andere Formen der nicht-inhaltlichen Daten – vielleicht sogar mehr über eine Einzelperson enthüllen können als der Inhalt selbst und verdienen daher einen gleichwertigen Schutz. Heute könnte jede dieser Informationsarten, für sich allein oder gemeinsam analysiert, die Identität einer Person, ihr Verhalten, ihre Verbindungen, ihren physischen oder gesundheitlichen Zustand, ihre Rasse, Hautfarbe, sexuelle Orientierung, nationale Herkunft oder Meinung enthüllen, oder den Aufenthaltsort einer Person mithilfe der Standortbestimmung, ihrer Bewegungen oder Interaktionen über einen Zeitraum[282] ermöglichen. Oder auch von allen Menschen an einem bestimmten Ort, zum Beispiel bei einer öffentlichen Demonstration oder anderen politischen Veranstaltung. Als Ergebnis sollten alle Informationen als »geschützte Informationen« angesehen werden, wenn sie sich aus der Kommunikation einer Person ergeben, diese beinhalten, reflektieren, oder über diese Person stattfinden, und nicht öffentlich verfügbar und leicht zugänglich für die allgemeine Öffentlichkeit sind. Ihnen sollte dementsprechend der höchste gesetzliche Schutz gewährt werden.

Bei der Beurteilung der Invasivität von staatlicher Kommunikationsüberwachung ist es notwendig, dass beides betrachtet

wird: sowohl das Potenzial der Überwachung, geschützte Informationen offenzulegen, sowie der Zweck, zu dem der Staat die Informationen sammelt. Kommunikationsüberwachung, die voraussichtlich zur Offenlegung von geschützten Informationen führt, die eine Person dem Risiko der Ermittlung, Diskriminierung oder Verletzung der Menschenrechte aussetzen kann, wird eine ernsthafte Verletzung des Rechts des Einzelnen auf Privatsphäre darstellen und außerdem die Nutzung anderer Grundrechte untergraben, unter anderem das Recht auf freie Meinungsäußerung, Versammlungsfreiheit und politische Partizipation. Dies liegt darin begründet, dass diese Rechte erfordern, dass Menschen frei von der abschreckenden Wirkung der staatlichen Überwachung kommunizieren können. Eine Festlegung sowohl der Art als auch der Einsatzmöglichkeiten der gesuchten Informationen wird somit in jedem Einzelfall notwendig.

Bei der Anwendung einer neuen Technik der Kommunikationsüberwachung oder der Ausweitung des Anwendungsbereichs einer bestehenden Technik sollte der Staat sicherstellen, ob die Informationen, die wahrscheinlich beschafft werden, in den Bereich der »geschützten Informationen« fallen, bevor er sie einholt, und sie zur Kontrolle der Justiz oder anderen demokratischen Kontrollorganen vorlegen. Bei der Beurteilung ob eine Information, die man mithilfe von Kommunikationsüberwachung erhalten hat, zu den »geschützten Informationen« gehört, sind sowohl die Form als auch der Umfang und die Dauer der Überwachung relevante Faktoren. Weil tiefgreifende oder systematische Überwachung private Informationen weit über seine Einzelteile hinaus offenbaren kann, kann es Überwachung von eigentlich nicht geschützten Informationen so invasiv machen, dass nun doch starker Schutz nötig wird[283].

Die Festlegung, ob der Staat Kommunikationsüberwachung von geschützten Informationen durchführen darf, muss im Einklang mit den folgenden Grundsätzen stehen.

Die Grundsätze

Gesetzmäßigkeit

Jede Beschränkung des Rechtes auf Privatsphäre muss gesetzlich vorgeschrieben sein. Der Staat darf in Abwesenheit eines bestehenden öffentlich verfügbaren Rechtsaktes, welcher Standards an Klarheit und Genauigkeit erfüllt, und der ausreichend sicherstellt, dass Einzelne eine Benachrichtigung erhalten haben und seine Anwendung abschätzen können, keine Maßnahmen einführen oder durchsetzen, die das Recht auf Privatsphäre beeinträchtigen. Angesichts der Geschwindigkeit des technologischen Wandels sollten Gesetze, die das Recht auf Privatsphäre beschränken, regelmäßig durch Instrumente eines partizipativen legislativen und behördlichen Prozesses überprüft werden.

Rechtmäßiges Ziel

Gesetze sollten nur Kommunikationsüberwachung durch spezifizierte Behörden erlauben, um ein legitimes Ziel zu erreichen, das einem für eine demokratische Gesellschaft notwendigen, überragend wichtigen Rechtsgut entspricht. Es darf keine Maßnahme angewendet werden, die auf der Grundlage von Rasse, Hautfarbe, Geschlecht, Sprache, Religion, politischer oder sonstiger Überzeugung, nationaler oder sozialer Herkunft, Vermögen, Geburt oder des sonstigen Status diskriminiert.

Notwendigkeit

Gesetze, die Kommunikationsüberwachung durch den Staat erlauben, müssen die Überwachung darauf beschränken, was zweifellos und nachweislich notwendig ist, um das legitime Ziel zu erreichen. Kommunikationsüberwachung darf nur durchgeführt werden, wenn es das einzige Mittel zur Erreichung eines rechtmäßigen Ziels ist oder wenn es das Mittel unter mehreren ist, welches eine Menschenrechtsverletzung am unwahrscheinlichsten macht. Der Nachweis der Begründung dieser Rechtfertigung in gerichtlichen sowie in Gesetzgebungsverfahren ist vom Staat zu leisten.

Angemessenheit

Jeder Fall der gesetzlich autorisierten Kommunikationsüberwachung muss geeignet sein, um das spezifische legitime Ziel, welches festgelegt wurde, zu erfüllen.

Verhältnismäßigkeit

Kommunikationsüberwachung sollte als hochgradig eindringende Handlung angesehen werden, die in das Recht auf Privatsphäre und die Freiheit der Meinungsäußerung eingreift und die Grundlagen einer demokratischen Gesellschaft bedroht. Entscheidungen über Kommunikationsüberwachung müssen die angestrebten Vorteile gegenüber den Schäden, die den Rechten des Einzelnen und anderen konkurrierenden Interessen zugefügt würden, abwägen und sollten eine Betrachtung der Sensibilität der Informationen und der Schwere der Rechtsverletzung auf Privatsphäre einbeziehen.

Dies erfordert insbesondere: Sollte ein Staat Zugang zu oder die Nutzung von geschützten Informationen anstreben, die durch Kommunikationsüberwachung im Rahmen einer strafrechtlichen Untersuchung gesammelt wurden, dann muss in der zuständigen, unabhängigen und unparteiischen gerichtlichen Entscheidung begründet sein, dass:

1. es eine hohe Wahrscheinlichkeit gibt, dass ein schweres Verbrechen begangen wurde oder begangen werden wird;
2. der Beweis eines solchen Verbrechens durch den Zugriff auf die geschützten Daten erhalten werden würde;
3. andere verfügbare und weniger invasive Ermittlungsmethoden ausgeschöpft sind;
4. die abgerufenen Informationen in vernünftiger Weise auf diejenigen begrenzt werden, die für die mutmaßliche Straftat relevant sind, und jede weitere gesammelte Information sofort vernichtet oder zurückgegeben wird; und
5. Informationen nur von der festgelegten Behörde abgerufen werden und nur für den Zweck verwendet werden, für den die Genehmigung erteilt wurde.

Wenn der Staat mit Kommunikationsüberwachung Zugang zu geschützten Informationen zu einem Zweck erlangen will, der eine Person nicht der Strafverfolgung, Ermittlung, Diskriminierung oder Verletzung der Menschenrechte aussetzt, muss der Staat einer unabhängigen, unparteiischen und zuständigen Behörde Folgendes nachweisen:

1. andere verfügbare und weniger invasive Ermittlungsmethoden wurden in Betracht gezogen;
2. die abgerufenen Informationen werden in vernünftiger Weise auf die relevanten begrenzt und jede zusätzlich gesammelte Information wird sofort vernichtet oder dem betroffenen Individuum zurückgegeben; und
3. Informationen werden nur von der festgelegten Behörde abgerufen und nur für den Zweck verwendet, für den die Genehmigung erteilt wurde.

Zuständige gerichtliche Behörden

Bestimmungen in Bezug auf die Kommunikationsüberwachung müssen von zuständigen gerichtlichen Behörden, die unparteiisch und unabhängig sind, festgelegt werden. Die Behörde muss:

1. getrennt sein von der Behörde, welche die Kommunikationsüberwachung durchführt,
2. vertraut sein mit den relevanten Themen und fähig sein, eine gerichtliche Entscheidung über die Rechtmäßigkeit der Kommunikationsüberwachung, die benutzte Technologie und Menschenrechte zu treffen, und
3. über entsprechende Ressourcen verfügen, um die ihr übertragenen Aufgaben auszuführen.

Rechtsstaatliches Verfahren

Ein rechtsstaatliches Verfahren verlangt, dass Staaten die Menschenrechte jedes Einzelnen respektieren und garantieren, indem sie rechtmäßige Prozesse zusichern, die jegliche Beeinträchtigung der

Menschenrechte ordnungsgemäß und gesetzlich spezifiziert regeln, die konsistent durchgeführt werden und die der allgemeinen Öffentlichkeit zugänglich sind. Insbesondere bei der Bestimmung seiner oder ihrer Menschenrechte hat jeder innerhalb einer angemessenen Frist das Recht auf ein faires und öffentliches Verfahren vor einem unabhängigen, zuständigen und unparteiischen rechtmäßig gegründeten Gericht[284], außer in Notfällen, wenn für Menschenleben Gefahr in Verzug ist. In solchen Fällen muss innerhalb einer vernünftigen und realisierbaren Frist eine rückwirkende Autorisierung eingeholt werden. Alleinig das Risiko der Flucht oder der Zerstörung von Beweismitteln soll niemals als ausreichend für eine rückwirkende Autorisierung angesehen werden.

Benachrichtigung des Nutzers

Personen sollten über die Entscheidung der Autorisierung einer Kommunikationsüberwachung informiert werden. Es sollten ausreichend Zeit und Informationen zur Verfügung gestellt werden, so dass die Person die Entscheidung anfechten kann. Des Weiteren sollte sie Zugang zu dem Material bekommen, welches für den Antrag der Autorisierung vorgelegt wurde. Eine Verzögerung der Benachrichtigung ist nur unter folgenden Bedingungen gerechtfertigt:

4. Die Benachrichtigung würde den Zweck, für den die Überwachung genehmigt ist, ernsthaft gefährden oder es besteht eine unmittelbare Gefahr für Menschenleben, oder
5. Die Erlaubnis einer Verzögerung der Benachrichtigung wird durch die zuständige Justizbehörde zum Zeitpunkt der Genehmigung der Überwachung erteilt; und
1. Die betroffene Person wird benachrichtigt, sobald die Gefahr aufgehoben ist, oder innerhalb einer vernünftigen realisierbaren Frist, je nachdem, welches zuerst zutrifft, aber in jeden Fall zu dem Zeitpunkt ,zu dem die Kommunikationsüberwachung abgeschlossen ist. Die Verpflichtung zur Benachrichtigung liegt beim Staat, aber in dem Fall, dass der Staat dem nicht nachkommt, sollten Kommunikationsdienstleister die Freiheit haben, Personen über die

Kommunikationsüberwachung freiwillig oder auf Anfrage zu benachrichtigen.

Transparenz

Staaten sollten bezüglich der Nutzung und des Umfangs der Techniken und Befugnisse der Kommunikationsüberwachung transparent sein. Sie sollten mindestens die gesammelten Informationen über die Anzahl der genehmigten und abgelehnten Anfragen, eine Aufschlüsselung der Anfragen nach Dienstanbieter und nach Ermittlungsart und -zweck veröffentlichen. Staaten sollten Personen genügend Informationen liefern, um zu gewährleisten, dass sie den Umfang, die Art und Anwendung der Gesetze, welche die Kommunikationsüberwachung erlauben, verstehen. Staaten sollten Dienstanbieter befähigen, die von ihnen angewendeten Maßnahmen zu veröffentlichen, wenn sie staatliche Kommunikationsüberwachung bearbeiten, an diesen Prozessen festzuhalten und Berichte der staatlichen Kommunikationsüberwachung zu veröffentlichen.

Öffentliche Aufsicht

Staaten sollten unabhängige Aufsichtsmechanismen schaffen, die Transparenz und Verantwortung der Kommunikationsüberwachung gewährleisten[285]. Aufsichtsmechanismen sollten die Befugnis gewähren, auf alle potenziell relevanten Informationen über staatliche Maßnahmen, wenn notwendig auch auf geheime oder als Verschlusssachen gekennzeichnete Informationen, zuzugreifen; zu beurteilen, ob der Staat seine rechtmäßigen Fähigkeiten legitim nutzt; zu beurteilen, ob der Staat die Informationen über den Einsatz und den Umfang der Techniken und Befugnisse der Kommunikationsüberwachung transparent und genau veröffentlicht hat; und regelmäßige Berichte und andere für die Kommunikationsüberwachung relevante Informationen zu veröffentlichen. Unabhängige Kontrollmechanismen sollten in Ergänzung zur Aufsicht geschaffen werden, die über einen anderen Teil der Regierung bereits zur Verfügung steht.

Integrität der Kommunikation und der Systeme

Um die Integrität, Sicherheit und Privatsphäre der Kommunikationssysteme zu gewährleisten und in Anerkennung der Tatsache, dass Abstriche bei der Sicherheit für staatliche Zwecke fast immer die Sicherheit im Allgemeinen infrage stellen, sollten Staaten die Dienstleister oder Hardware- oder Softwarehändler nicht zwingen, Überwachungs- oder Beobachtungsfunktionen in ihre Systeme einzubauen oder bestimmte Informationen nur für Zwecke der staatlichen Überwachung zu sammeln oder zu speichern. A-priori-Vorratsdatenspeicherung oder -Sammlung sollte nie von Dienstleistern gefordert werden. Personen haben das Recht, sich anonym zu äußern; Staaten sollten daher auf die zwingende Identifizierung der Nutzer als Voraussetzung für die Leistungserbringung verzichten[286].

Schutzmaßnahmen für die internationale Zusammenarbeit

Als Reaktion auf die Veränderungen der Informationsflüsse und Kommunikationstechnologien und -dienstleistungen kann es notwendig sein, dass Staaten Hilfe von einem ausländischen Dienstleister anfordern. Dementsprechend sollten die gemeinsamen Rechtshilfeverträge und andere Vereinbarungen, die von den Staaten eingegangen wurden, sicherstellen, dass in Fällen, in denen die Gesetze mehr als eines Staates für die Kommunikationsüberwachung angewendet werden können, derjenige verfügbare Standard mit dem höheren Schutzniveau für den Einzelnen angewendet wird. Wo Staaten Unterstützung für Zwecke der Strafverfolgung suchen, sollte der Grundsatz der beiderseitigen Rechenschaftspflicht angewendet werden. Staaten dürfen gemeinsame Rechtshilfeprozesse und ausländische Anfragen nach geschützten Informationen nicht nutzen, um inländische gesetzliche Beschränkungen der Kommunikationsüberwachung zu umgehen. Gemeinsame Rechtshilfeprozesse und andere Vereinbarungen sollten klar dokumentiert werden, öffentlich zugänglich sein und dem Schutz des fairen Verfahrens unterliegen.

Schutzmaßnahmen gegen unrechtmäßigen Zugang

Die Staaten sollten Gesetze erlassen, welche illegale Kommunikationsüberwachung durch öffentliche oder private Akteure kriminalisieren. Die Gesetze sollten ausreichende und erhebliche zivil- und strafrechtliche Sanktionen, Schutz für Whistleblower und Wege für die Wiedergutmachung von Betroffenen enthalten. Die Gesetze sollten vorsehen, dass alle Informationen, welche in einer Weise gesammelt wurden, die mit diesen Grundsätzen unvereinbar ist, in einem Verfahren als Beweise unzulässig sind, genauso wie Beweise, die von solchen Informationen abgeleitet sind. Die Staaten sollten außerdem mit der Maßgabe Gesetze erlassen, dass das durch Kommunikationsüberwachung gesammelte Material zerstört oder der Person zurückgegeben werden muss, nachdem es seinen Zweck erfüllt hat.

Supergrundrecht

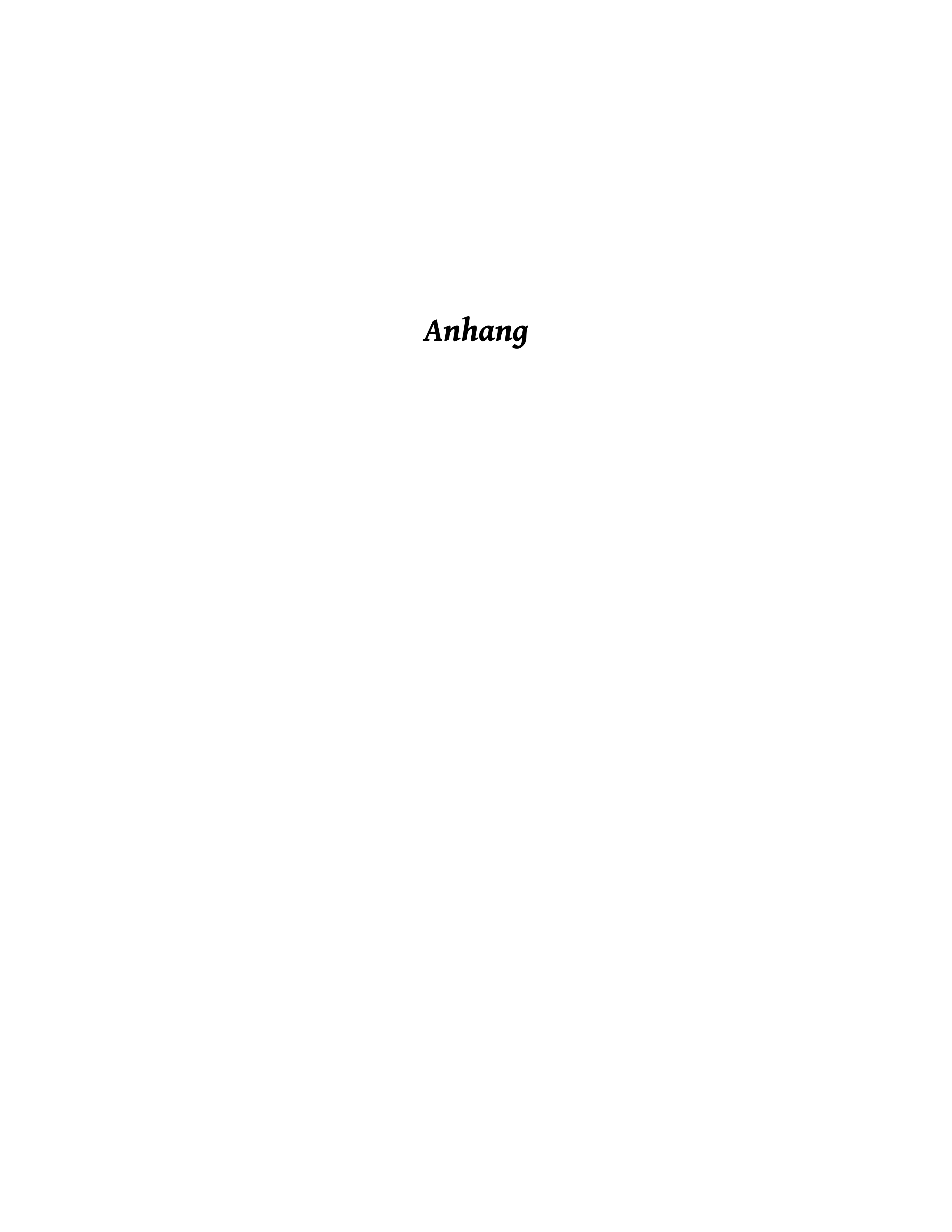
Kai Biermann

Grundrechte heißen Grundrechte, weil sie allem zugrunde liegen, was wir unter dem Begriff Rechtsstaat verstehen. Sie sind die Basis, das Fundament. So etwas muss man sprachlich nicht überhöhen, denn was kann wichtiger sein als der Boden, auf dem alles ruht? Eben. Innenminister Hans-Peter Friedrich hat trotzdem versucht, den Begriff zum S. zu übertreiben. »Sicherheit ist ein Supergrundrecht«, hat er nach einer Sitzung des Parlamentarischen Kontrollgremiums des Bundestages gesagt[287]. Sie sei im Vergleich mit anderen Rechten herauszuheben. Friedrich muss also einen Grund (haha) dafür gehabt haben, eine Hyperbel zu verwenden. Hatte er auch. Er wollte verschleiern, dass er erstens nicht die Sicherheit der Bürger meint und dass Sicherheit zweitens gar kein Grundrecht ist. Unsere Grundrechte sind sogenannte Abwehrrechte: Sie sollen den einzelnen und damit per se schwachen Bürger vor der Macht des Staates und seiner Organe schützen. Daher ist im Grundgesetz[288] oft von Freiheit die Rede, aber kaum von Sicherheit. Die Sicherheit kommt in all den Artikeln nur sechs Mal vor und jedes Mal geht es dabei um die Sicherheit des Staates, nie um die der Bürger. Die Freiheit hingegen wird im Grundgesetz 35 Mal erwähnt und gemeint ist immer die Freiheit des Einzelnen. Friedrichs Behauptung war also eine Lüge, die mit einer noch größeren Lüge kaschiert werden sollte. Eine klassische Taktik. Roland Koch hat sie berühmt gemacht, als er nicht nur Aufklärung versprach, sondern gleich *brutalstmögliche Aufklärung*[289] und nichts davon ernst meinte. Der Innenminister geht sogar noch weiter und dreht das gesamte Grundgesetz um. Denn dadurch, dass er Sicherheit im Zusammenhang mit den Grundrechten nennt, suggeriert er, es gehe um die Sicherheit der Bürger. Allerdings sagte Friedrich seinen Satz als Rechtfertigung eines Überwachungsprogramms. Es geht also darum, dass der Staat seine Bürger besser beobachten kann, um seine Informationshoheit und seine Macht zu sichern.

Lustigerweise hat Friedrich mit seiner kurzen Bemerkung nicht nur das Grundgesetz verdreht, sondern auch gleich noch belegt, dass er es gar nicht kennt. Denn es gibt tatsächlich ein Supergrundrecht[290], ein Grundrecht also, das über allen anderen steht: Es ist die Menschenwürde. Sie ist das einzige Grundrecht, das nicht durch Gesetze eingeschränkt werden kann, sie ist, wie es im Text heißt, »unantastbar«[291]. Und wollen Sie noch einen interessanten Fakt dazu hören? Aus eben dieser Menschenwürde ist das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[292] abgeleitet, das besagt, dass man darauf vertrauen können muss, von den eigenen technischen Geräten nicht überwacht zu werden.

Mit herzlichem Dank an die[293] fleißigen[294] Einsender[295].

Dieser Text ist zuerst am 29. Juli 2013 im Blog neusprech.org *erschienen*[296]*.*



Anhang

Autorinnen- und Autorenverzeichnis

Erik Albers ist Politikwissenschaftler und Aktivist. Er arbeitet bei der Free Software Foundation Europe im Policy Team und als Fellowship Coordinator. Als Politikwissenschaftler interessiert er sich für Demokratisierung, Partizipation und Meinungsfreiheit. (Twitter: @3albers)

Renata Avila Pinto ist Anwältin für Urheberrecht. Sie ist bei Creative Commons Guatemala als Projektleiterin tätig. Momentan arbeitet sie an Fällen zu internationalen Menschenrechten und als unabhängige Forscherin an Themen der Privatsphäre, Zugang zu Wissen und Redefreiheit für das Cyberstewards Netword, Citizen Lab, Universität Toronto. Sie ist Mitglied des Web Index Science Council und von Congreso Transparente. (Twitter: @avilarenata)

Markus Beckedahl betreibt seit 2002 netzpolitik.org. Er ist Mitgründer der newthinking GmbH, Mitgründer der re:publica-Konferenzen und Vorsitzender des Digitale Gesellschaft e.V. Er war Mitglied in der Enquete-Kommission Internet und digitale Gesellschaft im Deutschen Bundestag und ist Mitglied im Medienrat der Landesmedienanstalt Berlin-Brandenburg (MABB). (Twitter: @netzpolitik)

Yochai Benkler ist Juraprofessor an der Harvard Law School und Kodirektor des Berkman Center for Internet & Society der Harvard Universität. Er beschäftigt sich unter anderem mit Netzwerkproduktion und Urheberrecht. (Twitter: @YochaiBenkler)

Benjamin Bergemann studiert Politikwissenschaft in Berlin. Er interessiert sich besonders für Datenschutz, Überwachung und das große Ganze der Informationsgesellschaft. Benjamin ist Autor bei netzpolitik.org und engagiert sich im Digitale Gesellschaft e.V.

Kai Biermann ist studierter Psychologe und hat schon für die Berliner Zeitung, Financial Times Deutschland, die taz und viele andere Zeitungen geschrieben. Seit 2009 ist er bei ZEIT ONLINE zuständig für die Themen Internet, Datenschutz und Netzpolitik. Er betreibt

außerdem den neusprech.org Blog, zusammen mit Martin Haase. (Twitter: @kaibiermann)

Caspar Bowden war bis 2011 Microsofts Chief Privacy Adviser und ist nun unabhängiger Forscher, Rechtsanwalt und Aktivist für Datenschutzrecht. (Twitter: @CasparBowden)

Ian Brown ist stellvertretender Direktor des Cyber Security Centers der Universität von Oxford und Forschungsbeauftragter des Oxford Internet Instituts. Sein neuestes Buch ist *Regulating Code: Good Governance and Better Regulation in the Information Age* (mit Christopher T. Marsden) (Twitter: @IanBrownOII)

Andreas Busch ist Professor für Vergleichende Politikwissenschaft und Politische Ökonomie an der Georg-August-Universität Göttingen und Leiter der AG Netzpolitik am Institut für Politikwissenschaft. Zu seinen Arbeitsschwerpunkten gehören die vergleichende Staatstätigkeitsforschung mit Schwerpunkt Analyse von Regulierung sowie die Netzpolitik. Gegenwärtig leitet er im Rahmen eines Forschungsverbundes ein mehrjähriges Projekt über »Netzsperren in liberalen Demokratien« (2012-2015). Er ist Mitglied des Editorial Board der Zeitschrift *Policy and Internet* und stellvertretender Direktor des *Göttingen Centre for Digital Humanities*.

Johannes Caspar ist hamburgischer Beauftragter für Datenschutz und Informationsfreiheit sowie Rechtswissenschaftler mit besonderen Schwerpunkten im Bereich des öffentlichen Rechts und der Rechtsphilosophie.

Gabriella Coleman ist Inhaberin des Lehrstuhls für Scientific and Technological Literacy am Institut für Kunstgeschichte und Kommunikationswissenschaften der McGill University in Montreal, Kanada. (Twitter: @BiellaColeman)

Ot van Daalen war bis zum 1. Oktober 2013 Direktor von Bits of Freedom, einer niederländischen Organisation für digitale Rechte. Momentan arbeitet er als Jurist bei Bits of Freedom und wird im nächsten Jahr seine eigene Anwaltskanzlei gründen.

Kirsten Fiedler arbeitet bei European Digital Rights als Advocacy Manager. Ein Europastudiengang führte sie nach Liverpool, Aix-en-Provence und Köln, jetzt bloggt sie auf vasistas-blog.net und netzpolitik.org und ist aktiv bei der NURPA (Net Users' Rights Protection Association) in Belgien. Kirsten ist Schatzmeisterin des Digitale Gesellschaft e. V. (Twitter: @Kirst3nF)

Georg C. F. Greve ist seit fast 20 Jahren im Bereich der digitalen Gesellschaft aktiv als Autor und Sprecher im GNU Projekt, Gründungspräsident der Free Software Foundation Europe (FSFE) und in den letzten Jahren als CEO der Kolab Systems AG, einem reinen Open Source Anbieter. Für seine Verdienste wurde er 2009 mit dem Bundesverdienstkreuz am Bande ausgezeichnet.

Richard Gutjahr ist freier Journalist und Blogger. Er moderiert beim Bayerischen Fernsehen und hat eine eigene Kolumne in der Münchner Abendzeitung. Für seine journalistischen Leistungen im Netz wurde er dieses Jahr für den Grimme Online Award nominiert. (Twitter: @gutjahr)

Dirk Heckmann lehrt und forscht an der Universität Passau und der Zeppelin Universität Friedrichshafen. Der Internetrechtsexperte ist Mitglied des Bayerischen Verfassungsgerichtshofs und wirkt als Sachverständiger auf dem Nationalen IT-Gipfel der Bundesregierung sowie im CSU Netzrat. (Twitter: @elawprof)

Stefan Heumann studierte Politikwissenschaften an der Freien Universität Berlin, der Université de Provence in Aix-en-Provence und der University of Pennsylvania in Philadelphia. Von 2009 bis Ende 2010 unterrichtete Stefan Heumann als Assistant Professor an der University of Northern Colorado zu den Themenfeldern Globalisierung, vergleichende Policy Analyse und amerikanische Politik. In seiner Forschung setzte er sich insbesondere mit internationalen Einflüssen auf die Entwicklung des amerikanischen Staates auseinander. Von 2011 bis 2013 koordinierte Stefan Heumann die Öffentlichkeits- und Programmarbeit des US-Generalkonsulats in Hamburg. (Twitter: @St_Heumann)

Arne Hintz ist Dozent an der Cardiff School of Journalism, Media and Cultural Studies und Programmdirektor des Masterstudiengangs Journalism, Media and Communications. Seine Forschung konzentriert sich auf digitalen Aktivismus, Citizen Media, Globalisierung und technologischen Wandel. (Twitter: @arne_hz)

Christian Humborg ist Geschäftsführer von Transparency International Deutschland e.V. Die Antikorruptionsorganisation hat gemeinsam mit der Vereinigung Deutscher Wissenschaftler und der deutschen Sektion der IALANA den diesjährigen Whistleblowerpreis an den US-Amerikaner Edward J. Snowden verliehen. (Twitter: @chumborg)

Rikke Frank Jørgensen ist Beraterin des Dänischen Instituts für Menschenrechte und externe Dozentin des »International Master on Communication and Globalisation« an der Roskilde Universität in Dänemark. Außerdem ist sie Expertin für die Arbeitsgruppe »Rechte der Internet Nutzer« des Europarats. Ihr neuestes Buch heißt »Framing the Net: The Internet and Human Rights«.

Jan-Peter Kleinhans ist seit Juli 2013 Praktikant bei netzpolitik.org. In Deutschland wurde er zum Wirtschaftsinformatiker (BSc.), in Schweden zum Soziologen (MSc.) und zwischendurch hat er als Teamcoach und Präsentationstrainer gearbeitet. Sein Herz schlägt für den Datenschutz, die Privatsphäre und ein freies Internet, das ihn täglich überrascht, schockiert und zum Schmunzeln bringt. (Twitter: @jpkleinhans)

Torsten Kleinz ist freier Journalist und berichtet über das Internet und seine Auswirkungen auf die Gesellschaft und die Einflüsse der Gesellschaft auf das Netz.

Constanze Kurz ist promovierte Informatikerin. Sie forscht als wissenschaftliche Projektleiterin an der Hochschule für Technik und Wirtschaft in Berlin am Forschungszentrum »Kultur und Informatik«. Ehrenamtlich ist sie Sprecherin des Chaos Computer Clubs.

Daniel Leisegang ist Redakteur bei der politischen Monatszeitschrift »Blätter für deutsche und internationale Politik«. Er wurde 1978 in Unna/Westf. geboren und hat Politikwissenschaften, Germanistik und

Philosophie in Frankfurt a.M., Münster und Galway (Irland) studiert. (Twitter: @dleisegang)

Lorenz Matzat lebt und arbeitet als Journalist, Unternehmer und Medienpädagoge in Berlin. Seit Ende 2010 betreibt er mit zwei Partnern die Datenjournalismusagentur OpenDataCity | Die Datengestalter. Im Frühjahr 2011 gründete er zudem die Lokaler UG, die ein kartenbasiertes Daten- und Infosystem entwickelt. Er arbeitet als Journalismustrainer und referiert zu Datenjournalismus und Open Data. (Twitter: @lorz)

Andre Meister ist Sozialwissenschaftler und Systemadministrator. Er begleitet diverse netzpolitische Zusammenhänge wie AK Vorrat, AK Zensur oder CCC und ist Mitgründer des Digitale Gesellschaft e. V. Anfang 2012 konnte Andre das Bloggen auf netzpolitik.org zu seinem Beruf machen. (Twitter: @andre_meister)

Erich Moechel studierte amerikanische, deutsche und englische Literatur in Wien, war von 1999-2006 Ressortleiter des IT-Nachrichtenkanals futurezone.ORF.at. Seit 2010 schreibt er auf fm4.ORF.at und hat regelmäßig Auftritte als Experte in den Radio- und TV-Kanälen des ORF. Moechel ist Mitgründer der quintessenz (Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter), der Internationalen Big Brother Awards und Mitglied des International Board of Advisors von Privacy International.

Glyn Moody ist Journalist, Blogger und Redner. Jede Woche schreibt er für Techdirt über digitale Rechte und geistige Monopole und auf seinem Blog »opendotdotdot« über Open Source, Open Data und Open Culture. Sein Buch »Rebel Code: Linux and the Open Source Revolution« wurde 2001 veröffentlicht und ist die einzige detaillierte Geschichte freier Software, die bis heute verfasst wurde. (identi.ca: glynmoody@identi.ca, Twitter: @glynmoody)

Annette Mühlberg leitet das Referat E-Government, Neue Medien der Vereinten Dienstleistungsgewerkschaft (ver.di). Sie ist Vorstandsmitglied der europäischen Internetnutzerorganisation der Internet Corporation for Assigned Names and Numbers (ICANN); zuvor

war sie Vorsitzende des Internetnutzergremiums auf globaler Ebene. Für ver.di und den deutschen zivilgesellschaftlichen Koordinierungskreis war Annette Mühlberg aktiv beim Weltgipfel zur Informationsgesellschaft (WSIS). Sie war Sachverständige der Enquete-Kommission *Internet und digitale Gesellschaft* des Deutschen Bundestages.

Pranesh Prakash ist Policy Director des indischen Zentrums für Internet und Gesellschaft. In seiner Forschung beschäftigt er sich vor allem mit Urheberrechtsreformen, Open Access und Open Data, als auch Meinungsfreiheit und dem Schutz der Privatsphäre im Internet. (Twitter: @pranesh_prakash)

Frank Rieger ist technischer Geschäftsführer eines Unternehmens für Kommunikationssicherheit. Seit 1990 ist er einer der Sprecher des Chaos Computer Clubs. Zusammen mit Constanze Kurz veröffentlichte er das Buch »Die Datenfresser: Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen« (S. Fischer). (Twitter: @frank_rieger)

Katitza Rodriguez ist Direktorin für internationales Recht bei der Electronic Frontier Foundation. Ihr Augenmerk liegt auf dem Schutz der Privatsphäre im internationalen Kontext, Überwachung durch Regierungen und internationale Datenflüsse. (Twitter: @txitua)

Anne Roth, Berlin, Netz- und Medienaktivistin, Bloggerin (annalist.noblogs.org, gelegentlich netzpolitik.org), Researcher beim Tactical Technology Collective (tacticaltech.org). Ihre Themen sind Innenpolitik, Netzpolitik, Medien und Feminismus, außerdem Digitale Sicherheit. (Mail: annalist@riseup.net, Twitter: @annalist, englisch: @Anne_Roth)

Alexander Sander arbeitet für Martin Ehrenhauser, Mitglied des Europäischen Parlaments, und hat die Initiative NoPNR! gegründet. Er ist Mitglied bei Digitale Gesellschaft e.V. und Individual Observer bei EDRi. Er beschäftigt sich mit den Themen Innere Sicherheit, Datenschutz und Netzpolitik. (Twitter: @lexelas)

Peter Schaar ist diplomierter Volkswirt und seit dem 17. Dezember 2003 Bundesbeauftragter für den Datenschutz, seit dem 1. Januar 2006 auch Bundesbeauftragter für die Informationsfreiheit. Peter Schaar (geb. 1954) hatte zuvor ein Datenschutzberatungsunternehmen gegründet und bis 2002 das Amt des stellvertretenden Dienststellenleiters beim hamburgischen Beauftragten für den Datenschutz bekleidet. Für sein Buch »Das Ende der Privatsphäre« erhielt Schaar 2008 den Preis der Friedrich-Ebert-Stiftung»Das politische Buch«. Zudem unterrichtet er als Lehrbeauftragter an der Fakultät für Mathematik, Informatik und Naturwissenschaften der Universität Hamburg. (Twitter: @Peter_Schaar)

Bruce Schneier schreibt über Sicherheit, Technologie und Menschen. Sein letztes Buch ist »Liars and Outliers: Enabling the Trust That Society Needs to Thrive«. Er arbeitet für den Guardian an anderen NSA-Berichten. (Twitter: @schneierblog)

Ben Scott ist Senior Advisor des Open Technology Institute der New America Foundation in Washington DC und Visiting Fellow bei der Stiftung Neue Verantwortung in Berlin. Zuvor war er Berater für Innovation beim Außenministerium der Vereinigten Staaten, wo er an der Kreuzung von Technologie- und Außenpolitik tätig war.

Edward Snowden wurde als Whistleblower bekannt. Seine Enthüllungen gaben Einblicke in das Ausmaß der weltweiten Überwachungs- und Spionagepraktiken internationaler Geheimdienste. Er war technischer Mitarbeiter der US-amerikanischen Geheimdienste CIA und NSA. Bis Mai 2013 arbeitete er im Auftrag der NSA als Systemadministrator für das Beratungsunternehmen Booz Allen Hamilton.

Thomas Stadler ist Fachanwalt für IT-Recht und für gewerblichen Rechtsschutz in Freising. Er bloggt unter internet-law.de über Internetrecht und Bürgerrechte im digitalen Zeitalter. (Twitter: @RAStadler)

Felix Stalder ist Professor für Digitale Kultur und Theorien der Vernetzung in Zürich, Vorstandsmitglied des World Information

Institute in Wien und langjähriger Moderator der internationalen Mailingliste *nettime*. Er forscht u.a. zu Urheberrecht, Freier Kultur, Privatsphäre und Suchtechnologien. (Twitter: @stalfel)

Richard Stallman ist ein US-amerikanischer Aktivist und Programmierer. Er ist Befürworter und Entwickler Freier Software und Gründer des GNU-Projekts (zur Schaffung eines Freiheiten-gewährenden Betriebssystems). Stallman ist ursprünglicher Entwickler des GNU C-Compilers, des GNU Debuggesr und diverser anderer Software.

Moritz Tremmel studiert Politikwissenschaft, Soziologie und Rechtswissenschaft an der Universität Tübingen. Er schreibt zum Themenkomplex Datenschutz, Überwachung und Kontrolle wissenschaftliche Arbeiten und Artikel. Außerdem hält er Workshops und Vorträge zum Thema. Moritz Tremmel ist Teil des Forschernetzwerks surveillance-studies.org, bloggt bei netzpolitik.org und ist Mitglied des Vereins Digitale Gesellschaft.

Thilo Weichert ist Landesbeauftragter für Datenschutz Schleswig-Holstein und damit Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD).

Rüdiger Weis ist ein deutscher Diplom-Mathematiker und Kryptograph. Er lebt und arbeitet in Berlin-Wedding und ist Professor für Informatik an der Beuth-Hochschule für Technik Berlin. Er leitet die Kryptographie-Arbeitsgruppe *Cryptolabs* in Amsterdam. Seit vielen Jahren ist er aktives Mitglied des Chaos Computer Clubs. Zudem ist er Gründungsmitglied des Vereins Digitale Gesellschaft.

Krystian Woznicki gründete 1999 die Online-Zeitung Berliner Gazette, die er heute gemeinsam mit anderen Journalist/innen, Wissenschaftler/innen, Künstler/innen und Programmier/innen betreibt. (Twitter: @berlinergazette)

Jillian York ist Direktorin für internationale Meinungsfreiheit bei der Electronic Frontier Foundation. Sie schreibt regelmäßig Kolumnen für Global Voices Online und Al-Dschasira. (Twitter: @jilliancyork)

Jérémie Zimmermann ist Sprecher und Mitgründer der französischen Bürgerrechtsorganisation La Quadrature du Net und veröffentlichte 2012 zusammen mit Julian Assange das Buch »Cypherpunks: Freedom and the Future of the Internet«. (Twitter: @jerezim)

Abkürzungsverzeichnis

3GPP
: 3rd Generation Partnership Project; weltweite Kooperation von Standardisierungsgremien im Mobilfunk

ACLU
: American Civil Liberties Union; Amerikanische Bürgerrechtsunion

ACTA
: Anti-Counterfeiting Trade Agreement; Anti-Produktpiraterie-Handelsabkommen

AES
: Advanced Encryption Standard; symmetrisches Verschlüsselungsverfahren

AG
: Aktiengesellschaft

AK
: Arbeitskreis

AKW
: Atomkraftwerk

ALAC
: At-Large Advisory Committee

AP
: Associated Press; Nachrichtenagentur

ARD
: Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland

AT&T
: American Telephone and Telegraph; nordamerikanischer Telekommunikationskonzern

BBC
: British Broadcasting Corporation; britische Rundfunkanstalt

BDSG
: Bundesdatenschutzgesetz

BfV
: Bundesamt für Verfassungsschutz

BND
: Bundesnachrichtendienst; Auslandsgeheimdienst Deutschlands

BP
: British Petroleum / beyond petroleum; internationales Energieunternehmen

BSc.
: Bachelor of Science; akademischer Abschluss

BSI
: Bundesamt für Sicherheit in der Informationstechnik

BSIG
: Gesetz über das Bundesamtes für Sicherheit in der Informationstechnik

BVerfGE

Entscheidung des Bundesverfassungsgerichts

CALEA
: Communications Assistance to Law Enforcement Act; Kommunikations-Überwachungsgesetz der USA

CBDT
: Central Board of Direct Taxes

CCC
: Chaos Computer Club e.V.

CCTNS
: Crime criminal tracking network and systems; Netzwerk und System zur Verfolgung von Verbrechen in Indien

CCTV
: Closed Circuit Television; Überwachungskamerasysteme

CD
: Compact Disc; optischer Speicher

CD-ROM
: Compact Disc Read-Only Memory; optischer Speicher

CDU
: Christlich Demokratische Union Deutschlands

CEO
: Chief Executive Officer

CIA
: Central Intelligence Agency; Zentraler Nachrichtendienst der USA

CICIG
: Comisión Internacional contra la Impunidad en Guatemala; Internationalen Kommission zur Bekämpfung der Straflosigkeit in Guatemala

CID
: Crime Investigation Department

CIPPIC
: Canadian Internet Policy and Public Interest Clinic; Einrichtung der Universität vn Ottawa (Kanada) zur Entwicklung ausgewogener Regelwerke im Kontext neuer Technologien

CIS
: Center for Internet and Society; Zentrum für Internet und Gesellschaft

CMS
: Central Monitoring System; zentrales Überwachungssystem in Indien

COINTELPRO
: COunter INTELligence PROgram; geheimes Programm der US-Bundespolizei FBI

CPM
: Communist Party of India (Marxist); größte Linkspartei Indiens

CSU
: Christlich-Soziale Union in Bayern e.V.

DANA
: Datenschutz Nachrichten; Zeitschrift der Deutschen Vereinigung für Datenschutz (DVD)

DC
: District of Columbia

DDR
: Deutsche Demokratische Republik

DEA
: Drug Enforcement Administration; US-amerikanische Drogenbekämpfungsbehörde

DE-CIX
: German Commercial Internet Exchange; Internet-Knoten in Frankfurt am Main

DISA
: Defense Information Systems Agency; Militärgeheimdienst der USA

DLP
: Diskretes-Logarithmus-Problem

DNA
: Desoxyribonukleinsäure

DNI
: Inlandsgeheimdienst der USA

ECC
: Elliptische Kurven Kryptosystem

EDRi
: European Digital Rights; europäische Vereinigung von Bürgerrechtsorganisationen

EFF
: Electronic Frontier Foundation

EG
: Europäische Gemeinschaft

EGMR
: Europäischer Gerichtshof für Menschenrechte

ELENA
: elektronischer Einkommensnachweis

EMRK
: Europäische Menschenrechtskonvention

EPIC
: Electronic Privacy Information Center; Informationszentrum zur elektronischen Privatsphäre in Washington DC

ETSI
: European Telecommunications Standards Institute; Europäisches Institut für Telekommunikationsnormen

EU
: Europäische Union

EZLN
: Ejército Zapatista de Liberación Nacional; Zapatistische Armee der Nationalen Befreiung in Mexiko

FBI
: Federal Bureau of Investigation; Bundesamt für Ermittlung der USA

FCC
: Federal Communications Commission; Zulassungsbehörde für Kommunikationsgeräte in den USA

FISA
: Foreign Intelligence Surveillance Act; Gesetz zur Regelung der Aktivitäten der US-Nachrichtendienste

FISAAA
: Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008; Erweiterung des FISA von 2008

FISC
: United States Foreign Intelligence Surveillance Court; Gericht der Vereinigten Staaten betreffend die Überwachung der Auslandsgeheimdienste

FSFE
: Free Software Foundation Europe; Europäische Stiftung für Freie Software

G10
: Geltender Artikel zu Artikel 10 des Grundgesetzes; Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses

G20
: Gruppe der zwanzig wichtigsten Industrie- und Schwellenländer

GAU
: größter anzunehmender Unfall

GB
: Gigabyte; Datenmenge

GCHQ
: Government Communications Headquarters; Regierungskommunikationshauptquartier von Großbritannien

GEZ
: Gebühreneinzugszentrale; heute ARD ZDF Deutschlandradio Beitragsservice

GG
: Grundgesetz (der Bundesrepublik Deutschland)

GNU
: GNU’s Not Unix; GNU ist Nicht Unix, unixähnliches Betriebssystem

GnuPG
: GNU Privacy Guard; freies Kryptographiesystem

GPL
: GNU General Public License; Software-Lizenz für Freie Software

GPS
: Global Positioning System; globales Navigationssatellitensystem

GSM
: Global System for Mobile Communications; Standard für digitale Mobilfunknetze

HD
: High Definition; Hochauflösendes Video

HTTPS
: HyperText Transfer Protocol Secure; sicheres Hypertext-Übertragungsprotokoll

I2P
: Invisible Internet Project; unsichtbares Internet Projekt, Software-Projekt mit dem Ziel ein anonymes und pseudonymes Kommunikationsnetz zu schaffen

IALANA
: International Association of Lawyers against Nuclear Arms; Internationale Vereinigung von Anwälten gegen Atomwaffen

IBM
: International Business Machines Corporation; IT-Unternehmen aus den USA

ICC
: Interception of Communications Commissioner; Kommisar für Kommunikationsüberwachung Großbritanniens

ICCPR
: International Covenant on Civil and Political Rights; Internationale Pakt über bürgerliche und politische Rechte

ICT
: Information and Communication Technology; Informations- und Kommunikationstechnologien

IP
: Internet Protocol; Netzwerkprotokoll

IPv6
: Internet Protocol Version 6; Netzwerkprotokoll

ISA
: Intelligence Services Act; Gesetz über die Geheimdienste Großbritanniens

ISC
: Intelligence and Security Comittee; Geheimdienst- und Sicherheitsausschuss des britischen Parlaments

ISP
: Internet Service Provider; Internetanbieter

IT
: Informationstechnologie

KFZ
: Kraftfahrzeug

KGB
: Комитет государственной безопасности; In- und Auslandsgeheimdienst der Sowjetunion

MAD
: Amt für den militärischen Abschirmdienst; Nachrichtendienst der Bundeswehr

MI5
: Military Intelligence, Section 5 / Security Service, Inlandsgeheimdienst Großbritanniens

MI6
: Secret Intelligence Service; Geheimer Nachrichtendienst, Auslandsgeheimdienst Großbritanniens

MIKEY
: Multimedia Internet KEYing; Schlüsselaustauschprotokoll

MS
: Microsoft; Softwarehersteller aus den USA

MSc.
Master of Science; akademischer Abschluss

NATGRID
National Intelligence Grid; System zur Verknüpfung von Datenbanken der indischen Regierung

NATO
North Atlantic Treaty Organization; Organisation des Nordatlantikvertrags

NCP
Nationalist Congress Party; Partei in Indien

NGO
Non-Governmental Organization; Nichtregierungsorganisation

NIC
Network Information Center; Vergabestelle für Internet-Domains

NIS
Netz- und Informationssicherheit; Richtlinie der EU-Kommission

NIST
National Institute of Standards and Technology; Nationales Institut für Standards und Technologie

NJW
Neue Juristische Wochenschrift

NSA
National Security Agency; Nationale Sicherheitsbehörde der USA

NTRO
National Technical Research Organisation

OECD
Organisation for Economic Co-operation and Development; Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

OpenPGP
Open Pretty Good Privacy; Verschlüsselungsprogramm

ORF
Österreichische Rundfunk

OTI
Open Technology Institute; Institut für offene Technologie (USA)

OTR
Off-the-Record Messaging; Nachrichten-Verschlüsselung beim Instant Messaging

PC
Personal Computer

PFS
Perfect Forward Secrecy; perfekte vorwärts gerichtete Geheimhaltung, Eigenschaft von Schlüsselaustauschprotokollen

PKGr
Parlamentarische Kontrollgremium, Organ des Bundestages zur Kontrolle der Geheimdiensttätigkeit der Bundesregierung

PKGrG

Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes

PLCOB
: Privacy and Civil Liberties Oversight Board

PNR
: Passenger Name Record; Daten eines Fluggastes

PRISM
: Bedeutung unbekannt; Programm zur Überwachung und Auswertung elektronischer Medien und elektronisch gespeicherter Daten der NSA

PUCL
: People's Union of Civil Liberties

RC4
: Ron's Code 4; Verschlüsselungsverfahren

RC5
: Rivest Cipher 5; Verschlüsselungsverfahren

RFID
: Radio-Frequency Identification; Identifizierung mit Hilfe elektromagnetischer Wellen

RIPA
: Regulation of Investigatory Powers Act; Telekommunikationsgesetz in Großbritannien

RSA
: Rivest, Shamir und Adleman; assymetrisches Verschlüsselungsverfahren

SA3LI
: Arbeitsgruppe für Telekommunikationsüberwachung der 3GPP

SCL
: Society for Computers and Law; Gesellschaft für Computer und Recht in Großbritannien

SHA, SHA1-3
: Secure Hash Algorithm; Algorithmen für sichere Streuwerte

SIPRnet
: Secret Internet Protocol Router Network; Verbund von Computernetzwerken des Außen- und Verteidigungsministeriums der USA

SMS
: Short Message Service; Kurznachrichtendienst im Mobilfunk

SPD
: Sozialdemokratische Partei Deutschlands

SSL
: Secure Sockets Layer; alte Bezeichnung für Transport Layer Security

StGB
: Strafgesetzbuch

STOA
: Scientific and Technological Options Assessment Programme; Ausschuss zur Technikfolgenabschätzung des Europaparlaments

SWIFT
: Society for Worldwide Interbank Financial Telecommunication; internationale Genossenschaft der Geldinstitute zum Informationsaustausch

TAT-14
Transatlantic Telecommunications Cable no. 14; Transatlantisches Telefonkabel Nr. 14
TKG
Telekommunikationsgesetz
TLS
Transport Layer Security; Netzwerkprotokoll zur sicheren Übertragung von Daten
TPM
Trusted Platform Module; Chip deer Trusted Computing Group Spezifikation
TTIP
Transatlantic Trade and Investment Partnership; Transatlantisches Freihandelsabkommen (TAFTA) zwischen Nord-Amerika und Europa
TV
Television
UDHR
Universal Declaration of Human Rights; Allgemeine Erklärung der Menschenrechte
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UN
United Nations; Vereinte Nationen
USA PATRIOT Act
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001; Gesetz der USA zur Stärkung und Einigung Amerikas durch Bereitstellung geeigneter Instrumente, um Terrorismus aufzuhalten und zu blockieren
US(A)
United States (of America); Vereinigte Staaten (von Amerika)
VPN
Virtual Private Network; geschlossenes Netz innerhalb einer öffentlichen Netzwerk-Infrastruktur
WDR
Westdeutscher Rundfunk Köln
WLAN
Wireless Local Area Network; drahtloses lokales Netzwerk
WSIS
Weltgipfel zur Informationsgesellschaft
ZDF
Zweites Deutsches Fernsehen

[1] *Original-Rede; The WikiLeaks Supporters Forum; http://www.wikileaks-forum.com/news-and-supporters/335/snowden-wins-whistleblower-award-in-germany/22431/*

[2] http://www.zdnet.com/nsa-hunger-demands-29-petabytes-of-data-a-day-7000019255/

[3] Vgl. http://heise.de/-1970044

[4] Die Bedrohung, dass das öffentliche Mund-Aufmachen, etwa das Zeichnen einer Petition für den Erhalt der Grundrechte angesichts der NSA-Überwachung, sanktioniert wird, scheint bereits bittere Realität zu sein: Dem Schriftsteller Ilija Trojanow, der sich dem Aufruf angeschlossen und 2009 das Buch »Angriff auf die Freiheit« verfasst hatte, verweigerten die USA im September 2013 ohne Angaben von Gründen die Einreise aus Brasilien direkt am Flughafen Salvador da Bahia. Kafka lässt grüßen.

[5] Statt für die Einhaltung unserer Grundrechte einzutreten, werden sie als eine *»Idylle aus vergangenen Zeiten«* bezeichnet, so der CSU-Innenpolitiker Hans-Peter Uhl zum Grundrecht auf informationelle Selbstbestimmung; CDU/CSU und SPD fordern unbeeindruckt ihres Missbrauchspotentials die Wiedereinführung der Vorratsdatenspeicherung. Dass man auf die Verletzung der Grundrechte durch Geheimdienste politisch ganz anders reagieren kann, zeigte Brasiliens Präsidentin, Dilma Rousseff. In ihrer Rede vor der UN-Vollversammlung im September 2013 stellte sie klar:

... »...In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy. In the absence of the respect for sovereignty, there is no basis for the relationship among Nations. We face, Mr. President, a situation of grave violation of human rights and of civil liberties; of invasion and capture of confidential information concerning corporate activities, and especially of disrespect to national sovereignty. We expressed to the Government of the United States our disapproval, and demanded explanations, apologies and guarantees that such procedures will never

be repeated. Friendly governments and societies that seek to build a true strategic partnership, as in our case, cannot allow recurring illegal actions to take place as if they were normal. They are unacceptable. Brazil, Mr. President, will redouble its efforts to adopt legislation, technologies and mechanisms to protect us from the illegal interception of communications and data. My Government will do everything within its reach to defend the human rights of all Brazilians and to protect the fruits borne from the ingenuity of our workers and our companies ...«
http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf

[6] So zum Beispiel in Großbritannien: Im »Intelligence Service Act« von 1994 wird als Aufgabe der Geheimdienste auch der Erhalt des britischen »economic well-being« genannt wird.

[7] http://www.stopsurveillance.org/

[8] Im Rahmen der Diskussion um den Schutz der Netzneutralität wurde ein erster Anfang gemacht. Ziel muss es sein, das offene Internet zu erhalten, das Daten nur von A nach B transportiert und sich nicht auch eine Bevorzugung bestimmter Dienste. Eine solche positive Diskriminierung käme für Absender, Empfänger oder Inhalte interessiert. Dazu muss der Schutz der Netzneutralität festgelegt werden. Das bedeutet nicht nur, wie im Entwurf der EU Kommission vom September 2013 vorgesehen, den kompletten Ausschluss von Internet-Angeboten durch Telekommunikationsprovider oder ein willkürliches Sperren des Internetverkehrs zu verbieten, sondern einer inhaltlichen Vorzensur gleich, der zu begegnen, den Bürger/innen einen erheblichen organisatorischen und zusätzlichen finanziellen Aufwand abverlangen würde. Es muss endlich anerkannt werden, dass das Internet zu einer gemeinschaftlichen Infrastruktur geworden ist, die sowohl digitaler Markt als auch Teil öffentlicher Daseinsvorsorge ist (vgl. auch das »Berliner Manifest: Die Daseinsvorsorge in der Informationsgesellschaft stärken!« von ver.di:
http://www.governet.de/wp-content/uploads/2012/12/ver.di-Berliner_Manifest_de.pdf)

[9]Vgl. Gerald Santucci: Privacy in the Digital Economy: Requiem or Renaissance? http://www.privacysurgeon.org/blog/wp-content/uploads/2013/09/Privacy-in-the-Digital-Economy-final.pdf

[10]Siehe Initiativen wie stopsurveillance.org oder »Hamburger Erklärung zur Totalüberwachung«

[11]Vgl. https://www.eff.org/deeplinks/2013/10/nsa-making-us-less-safe

[12]Vgl. http://heise.de/-1973021

[13]Danke an Antje Schrupp für »Mein Problem mit Post-Privacy«, http://antjeschrupp.com/2011/11/09/mein-problem-mit-post-privacy/

[14]E-Mail made in Germany: Deutsche Telekom, Web.de und GMX machen SSL an und verkaufen das als »sicher«, Netzpolitik.org 9. 8. 13 https://netzpolitik.org/2013/e-mail-made-in-germany-deutsche-telekom-web-de-und-gmx-machen-ssl-an-und-verkaufen-das-als-sicher/

[15]Neues von Echelon, Spiegel Online, 21.5.99 http://www.spiegel.de/netzwelt/web/lauschangriff-neues-von-echelon-a-23279.html

[16]*faz.net; 10. August 2013, S. 31; Die neuen Krypto-Kriege; http://www.faz.net/aktuell/feuilleton/snowdens-maildienst-gibt-auf-die-neuen-krypto-kriege-12475864.html*

[17]verkürzter Auszug aus dem Buch »Der Informant«, Bob Woodward, Spiegel-Verlag

[18]*gutjahr.biz; 22. August 2013; http://gutjahr.biz/2013/08/prism-break-season-1/*

[19]*Berliner Gazette; 20. August 2013; http://berlinergazette.de/buerger-staat-edward-snowden-digitale-gegenwart/*

[20]*netzpolitik.org; Torsten Kleinz; Es ist keine Spähaffäre; 11. September 2013; https://netzpolitik.org/2013/es-ist-keine-spaehaffaere/*

[21] http://www.washingtonpost.com/wp-srv/special/national/black-budget/

[22] http://fm4.orf.at/stories/1725452/

[23] http://www.dradio.de/dkultur/sendungen/politischesfeuilleton/2264727/

[24] http://www.taz.de/Geheimdienst-an-der-Spree/!124577/

[25] http://www.slate.com/blogs/future_tense/2013/08/26/nsa_s_data_should_be_available_for_public_use.html

[26] Bauchmüller, Michael und Klaus Ott 2010: 173.000 Mitarbeiter überprüft, Süddeutsche Online, 10.05.2010, http://www.sueddeutsche.de/wirtschaft/datenaffaere-bei-der-deutschen-bahn-mitarbeiter-ueberprueft-1.478024

[27] Transparency International Deutschland 2009: Stellungnahme anlässlich des Berichts der Sonderermittler des Aufsichtsrates der Deutschen Bahn, 15.05.2009, http://www.transparency.de/Stellungnahme-zur-Deutschen-Ba.1444.0.html

[28] Obenhaus, Nils 2010: Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, in: Neue Juristische Wochenschrift, 63. Jg., Heft 10, S. 651-655.

[29] Humborg, Christian 2013: Der Kampf gegen Korruption im digitalen Zeitalter, in: Carl-Heinrich Bösling, Lioba Meyer und Thomas F. Schneider (Hg.), Lost in Cyber Space – Schreiben gegen Krieg im Zeitalter digitaler Medien, Göttingen, S. 49-58.

[30] Scott, Shane und Tom Bowman 1995: America's Fortress of Spies Series – National Security Agency, The Baltimore Sun, 03.12.1995, http://articles.baltimoresun.com/1995-12-03/news/1995337001_1_intelligence-agency-nsa-intelligence-national-security-agency

[31] Woolsey, R. James 2000: Ja, liebe Freunde, wir haben Euch ausgehorcht, Zeit Online, 30.03.2000, http://www.zeit.de/2000/14/200014.spionieren_.xml

[32] Transparency International 2009: Recommended draft principles for whistleblowing legislation, http://www.transparency.org/files/content/activity/2009_PrinciplesForWhistleblowingLegislation_EN.pdf

[33] Open Society Justice Initiative 2013: European Endorsement for Tshwane Principles on National Security and Right to Know, 24.06.2013, http://www.opensocietyfoundations.org/press-releases/european-endorsement-tshwane-principles-national-security-and-right-know

[34] Cloud Times: US Cloud Providers may lose 35$ billion due to PRISM http://cloudtimes.org/2013/08/16/us-cloud-providers-may-lose-35-billion-due-to-prism/

[35] The Washinton Post: Former NSA chief: 'Morally arrogant' Snowden will probably become an alcoholic http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/17/former-nsa-chief-morally-arrogant-snowden-will-probably-become-an-alcoholic/

[36] The Washington Post: Obama undergoes a philosophical shift on counterterrorism surveillance: http://www.washingtonpost.com/politics/obama-strives-for-pragmatic-compromises-on-counterterrorism-surveillance/2013/06/07/f8ee4302-cf88-11e2-8845-d970ccb04497_story.html

[37] EDRi: Questions on the draft Directive on Cybersecurity Strategy http://www.edri.org/edrigram/number11.1/cybersecurity-draft-directive-eu

[38] CCC: Trügerische Sicherheit: Der elektronische Personalausweis http://www.ccc.de/en/updates/2013/epa-mit-virenschutzprogramm

[39] Netzpolitik: Untersuchung: Vorratsdatenspeicherung ist ineffektiv https://netzpolitik.org/2011/untersuchung-vorratsdatenspeicherung-ist-ineffektiv/

[40] Netzpolitk: Geheimes Dokument zeigt die schmutzigen Tricks bei den SWIFT-Verhandlungen; https://netzpolitik.org/2009/geheimes-dokument-zeigt-die-schmutzigen-tricks-bei-den-swift-verhandlungen/

[41] Süddeutsche: »Wir wollen keinen Staat, der nur Konformisten hervorbringt«, http://www.sueddeutsche.de/bayern/datenschutzbeauftragter-zur-videoueberwachung-wir-wollen-keinen-staat-der-nur-konformisten-hervorbringt-1.1735146

[42] Süddeutsche: Anschläge, die keine waren http://www.sueddeutsche.de/politik/geheimdiensterkenntnisse-durch-prism-anschlagsplaene-die-keine-waren-1.1721889

[43] Schneier on Security: https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html

[44] NY Times: Secret Documents Reveal N.S.A. Campaign Against Encryption http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us&_r=0

[45] Brevini, Benedetta, Arne Hintz und Patrick McCurdy (2013) Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society, Palgrave MacMillan.

[46] Nolan, Hamilton (2013) 'The Vain Media Cynics of the NSA Story', Gawker 11 June 2013, http://gawker.com/the-vain-media-cynics-of-the-nsa-story-512575457

[47] Lobo, Sascha (2013) 'Staatliche Ueberwachung: Das Zeitalter des Pseudoprivaten beginnt jetzt', Spiegel Online 8. Oktober 2013,

http://www.spiegel.de/netzwelt/web/kolumne-sascha-lobo-zeitalter-des-pseudoprivaten-beginnt-a-926633.html

[48] Taibbi, Matt (2013) ‘As Bradley Manning Trial Begins, Press Predictably Misses the Point’, 6 June 2013, Rolling Stone, http://www.rollingstone.com/politics/blogs/taibblog/as-bradley-manning-trial-begins-press-predictably-misses-the-point-20130605

[49] Herman, Edward, und Noam Chomsky (1988) Manufacturing Consent, Pantheon Books.

[50] Blackhurst, Chris (2013) ‘Edward Snowden’s secrets may be dangerous. I would not have published them’, The Independent 13 October 2013, http://www.independent.co.uk/voices/comment/edward-snowdens-secrets-may-be-dangerous-i-would-not-have-published-them-8877404.html

[51] Rusbridger, Alan (2013) ‘David Miranda, schedule 7 and the danger that all reporters now face’, The Guardian 19 August 2013, http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters

[52] Benkler, Yochai (2013) ‘WikiLeaks and the Networked Fourth Estate’, in Benedetta Brevini, Arne Hintz und Patrick McCurdy (2013) Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society, Palgrave MacMillan, S. 11-34.

[53] Curdy, Patrick (2013) ‘From the Pentagon Papers to Cablegate: How the Network Society Has Changed Leaking’, in Benedetta Brevini, Arne Hintz und Patrick McCurdy (2013) Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society, Palgrave MacMillan, S. 123-145.

[54] Star, Alexander und Bill Keller (2011) Open Secrets: WikiLeaks, War and American Diplomacy, Grove Press.

[55] Taylor, Marisa und Jonathan S. Landai (2013) ‘Obama’s crackdown views leaks as aiding enemies of U.S.’, McClatchyDC 20 June 2013,

http://www.mcclatchydc.com/2013/06/20/194513/obamas-crackdown-views-leaks-as.html

[56] Banisar, David und Francesca Fanussi (2013) ‘WikiLeaks, Secrecy, and Freedom of Information: The Case of the United Kingdom’, in Benedetta Brevini, Arne Hintz und Patrick McCurdy (2013) Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society, Palgrave MacMillan, S. 178-190.

[57] Castells, Manuel (2009) Communication Power, Oxford University Press.

[58] Mitchell, Greg (2011) The Age of WikiLeaks, Sinclair Books.

[59] obo, Sascha (2013) ‘Staatliche Ueberwachung: Das Zeitalter des Pseudoprivaten beginnt jetzt’, Spiegel Online 8. Oktober 2013, http://www.spiegel.de/netzwelt/web/kolumne-sascha-lobo-zeitalter-des-pseudoprivaten-beginnt-a-926633.html

[60] Greenwald, Glenn (2013) ‘Fisa court oversight: a look inside a secret and empty process’, The Guardian 19 June 2013, http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy

[61] Huhne, Chris (2013) ‘Prism and Tempora: the cabinet was told nothing of the surveillance state’s excesses’, The Guardian 6 October 2013, http://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet-surveillance-state

[62] Jewell, John (2013) ‘Journalism under attack? The Guardian and press freedom’, Jomec Blog 21 August 2013, http://www.jomec.co.uk/blog/journalism-under-attack-the-guardian-and-press-freedom/

[63] The Guardian (17 October 2013) ‘Extent of spy agencies’ surveillance to be investigated by parliamentary body’, 17 October 2013, http://www.theguardian.com/uk-news/2013/oct/17/uk-gchq-nsa-surveillance-inquiry-snowden

[64]Goldsmith, HJack und Tim Wu (2006) Who Controls the Internet? Illusions of a Borderless World, Oxford University Press.

[65]Clinton, Hillary (2010), 'Remarks on Internet Freedom', US State Department 21 January 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm

[66]http://news.sky.com/story/1151959/mi5-chiefs-speech-on-terrorism-in-full

[67]Heumann, S., & Scott, B. (2013). Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany (p.17).

[68]https://netzpolitik.org/2013/fliegende-schweine-wie-die-westlichen-geheimdienste-verschluesselung-mit-man-in-the-middle-angriffen-aushebeln/

[69]Levinson-Waldman, R. (2013). WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA (p.88).

[70]http://www.csmonitor.com/2006/0901/p03s03-uspo.html

[71]http://www.slate.com/articles/technology/technology/2013/04/google_has_a_single_towering_obsession_it_wants_to_build_the_star_trek_computer.2.html

[72]*Gabriella Coleman, Author of Coding Freedom on the NSA Leaks; 23. August 2013; http://blog.press.princeton.edu/2013/08/23/gabriella-coleman-author-of-coding-freedom-on-the-nsa-leaks/*

[73]http://www.faz.net/aktuell/politik-im-datenzeitalter-was-die-spd-verschlaeft-12591683.html

[74]https://netzpolitik.org/2013/politik-unplugged-das-lobbyplag-datenschutz-ranking/

[75]https://netzpolitik.org/2013/innenausschuss-des-eu-parlaments-stimmt-am-21-oktober-ueber-datenschutzverordnung-ab/

[76] https://netzpolitik.org/2013/geheimer-haushalt-die-usa-geben-in-diesem-jahr-ueber-50-milliarden-dollar-fuer-ihre-geheimdienste-aus/

[77] Vgl. dazu die Empfehlungen der Artikel-29-Datenschutzgruppe: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, S. 41.

[78] Vgl. dazu die Untersuchung von Bits of Freedom zum legitimen Interesse: https://www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf

[79] Vgl. dazu den Bericht von Caspar Bowden für den Überwachungs-Untersuchungsausschuss des Innenausschusses des Europäischen Parlaments: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf, S. 30.

[80] https://netzpolitik.org/2012/mozilla-privacy-icons-komplexe-datenschutz-bestimmungen-in-einfachen-icons-visualisieren/

[81] Vgl. dazu die Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juli 2013: http://www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.9283.de

[82] *Wir werden jede Ressource, die wir zur Verfügung haben – jedes diplomatische Mittel, jedes Geheimdienstwerkzeug, jedes Strafverfolgungsinstrument, jeden finanziellen Einfluss und jede nötige Kriegswaffe – zur Zerstörung und Bekämpfung des globalen Terrornetzwerks nutzen.*, vgl. George Bush, Rede anlässlich der Gemeinsamen Sitzung des US-Kongresses vom 20. September 2001, online abrufbar unter http://www.npr.org/news/specials/americatransformed/reaction/010920.bushspeech.html)

[83] »*Erstens: Wir sind keinem Programm beigetreten, dass der US-Regierung – oder irgendeiner anderen Regierung – direkten Zugriff zu unseren Servern geben würde. Tatsache ist, dass die US-Regierung keinen direkten Zugriff oder*

ein »Back Door« zu den Informationen in unseren Datencentern hat. […] Zweitens: Wir geben Nutzerdaten nur an Regierung, wenn das rechtmäßig ist. […] Presseberichte, die nahelegen, dass Google unbeschränkten Zugang zu den Daten unserer Nutzer bietet, sind falsch […] vgl. Google Blog, What the …?, vom 7. Juni 2013, online abrufbar unter http://googleblog.blogspot.de/2013/06/what.html

[84] http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline

[85] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//DE

[86] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/1001/1001938/1001938en.pdf

[87] http://europa.eu/rapid/press-release_SPEECH-13-536_en.htm

[88] http://europa.eu/rapid/press-release_SPEECH-13-537_en.htm

[89] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130813_letter_to_vp_reding_final_en.pdf

[90] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/draft_programme_/draft_programme_en.pdf

[91] Vgl. http://www.bundestag.de/bundestag/gremien/pkgr

[92] Vgl. http://www.gesetze-im-internet.de/bundesrecht/pkgrg/gesamt.pdf

[93] Die Bundesregierung kann die Unterrichtung laut PKGrG jedoch verweigern, »soweit dies aus zwingenden Gründen des Nachrichtenzugangs oder aus Gründen des Schutzes von Persönlichkeitsrechten Dritter notwendig ist oder wenn der Kernbereich der exekutiven Eigenverantwortung betroffen ist«.

[94] Vgl. http://www.bundestag.de/bundestag/gremien/g10/mitglieder.html

[95]Vgl. Wolfgang Nešković, Geheimdienstkontrolle: PR statt Aufklärung,http://www.faz.net/aktuell/politik/geheimdienstkontrolle-pr-statt-aufklaerung-12496027.html

[96]http://isc.independent.gov.uk

[97]Vgl. Daniel Leisegang, Schöne neue Überwachungswelt, http://www.blaetter.de/archiv/jahrgaenge/2013/august/schoene-neue-ueberwachungswelt

[98]Vgl. »Flexible Laws and weak oversight give GCHQ room for manoeuvre«, http://www.theguardian.com/uk-news/2013/aug/02/gchq-laws-oversight-nsa; siehe dazu auch: George Monbiot, How can we invest our trust in a government that spies on us?, http://www.theguardian.com/commentisfree/2013/jun/24/how-trust-state-spies-citizens

[99]Vgl. Andrew Rosenthal, A Court Without Adversaries, http://takingnote.blogs.nytimes.com/2013/07/09/a-court-without-adversaries

[100]Vgl. Glenn Greenwald, Fisa Court Oversight: a Look Inside a Secret and Empty Process, http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy

[101]netzdebatte.bpb.de; Daniel Leisegang; 13. September 2013; https://www.bpb.de/dialog/netzdebatte/169068/geheimdienste-ausser-kontrolle-wer-ueberwacht-eigentlich-die-ueberwacher

[102]Denninger, E. 1990. ‘Der Präventions-Staat’, in: Denninger, E. (ed.), Der gebändigte Leviathan. Baden-Baden: Nomos, 33-49.

[103]Grimm, D. 1994. ‘Verfassungsrechtliche Anmerkungen zum Thema Prävention’, in: Die Zukunft der Verfassung. Frankfurt am Main: Suhrkamp, 197-220.

[104]Andreas, P. 2003. ‘Redrawing the Line: Borders and Security in the Twenty-First Century’, International Security, 28:2, 78-111.

[105] Kettl, D. F. 2004. System under stress. Homeland security and American politics. Washington, D.C.: CQ Press.

[106] American Civil Liberties Union 2004. The Surveillance-Industrial Complex:. How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society. New York (N.Y.): ACLU.

[107] Organisation for Economic Co-operation and Development, ed. 2004. The security economy. Paris: OECD.

[108] Broeders, D., und Hampshire, J. 2013. 'Dreaming of Seamless Borders:. ICTs and the Pre-Emptive Governance of Mobility in Europe', Journal of Ethnic and Migration Studies, 39:8, 1201-1218.

[109] 'The National DNA Database Annual Report 2011-2012'.

[110] Busch, A. 2010. 'Kontinuität statt Wandel. Die Innen- und Rechtspolitik der Großen Koalition', in: Egle, C. and Zohlnhöfer, R. (eds.), Die zweite Große Koalition. Eine Bilanz der Regierung Merkel 2005-2009. Wiesbaden: VS Verlag für Sozialwissenschaften, 401-430.

[111] Priest, D., und Arkin, W. M. 2011. Top secret America. The rise of the new American security state. New York: Little Brown and Co.

[112] Lyon, D. 2003. Surveillance after September 11. Cambridge: Polity Press.

[113] Katzenstein, P. J. 2003. 'Same War - Different Views: Germany, Japan, and Counterterrorism', International Organization, 57:4, 731-760.

[114] Katzenstein, P. J. 2003. 'Same War - Different Views: Germany, Japan, and Counterterrorism', International Organization, 57:4, 731-760.

[115] Zenko, M., und Cohen, M. A. 2012. 'Clear and Present Safety', Foreign Affairs, 91:2, 79-93.

[116] Independent Reviewer of Terrorism Legislation 2012. The Terrorism Acts in 2011. Report of the Independent Reviewer on the Operation of

the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006. Presented to Parliament pursuant to Section 36 of the Terrorism Act 2006. London.

[117] Genschel, P., und Zangl, B. 2008. 'Metamorphosen des Staates. Vom Herrschaftsmonopolisten zum Herrschaftsmanager', Leviathan, 36:3, 430-454.

[118] *Oxford Handbook of Transformations of the State; Hrsg. von Evelyne Huber, Stephan Leibfried, Matthew Lange, Jonah Levy, Frank Nullmeier und John Stephens (Oxford University Press 2014)*

[119] Die NSA bezeichnet US-Bürger, Fremde mit permanentem Wohnsicht, US-Unternehmen und Verbände von US-Bürgern oder Einwohnern als US-Personen. http://www.nsa.gov/sigint/faqs.shtml#sigint4

[120] https://it.ojp.gov/default.aspx?area=privacy&page=1286#contentTop

[121] http://www.theatlantic.com/technology/archive/2013/06/us-government-surveillance-bad-for-silicon-valley-bad-for-democracy-around-the-world/277335/

[122] Entsprechen der Bereitstellung der Geschäftsunterlagen in Abschnitt 215-50 U.S.C. § 1861(b)(2)(A)

[123] Siehe Charlie Savage, »N.S.A. Said to Search Content of Messages to and From U.S.«, »http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all&_r=2&

[124] http://business.time.com/2013/07/03/nsa-scandal-as-tech-giants-fight-back-phone-firms-stay-mum/

[125] http://www.theguardian.com/world/interactive/2013/jun/08/nsa-boundless-informant-data-mining-slides

[126] http://www.lawfareblog.com/wp-content/uploads/2013/06/Facts-on-the-Collection-of-Intelligence-Pursuant-to-Section-702.pdf

[127] http://www.nbcnews.com/technology/court-sides-yahoo-nsa-prism-data-collection-case-6C10651458

[128] http://www.theatlantic.com/technology/archive/2013/06/us-government-surveillance-bad-for-silicon-valley-bad-for-democracy-around-the-world/277335/

[129] Siehe beispielsweise: http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf

[130] https://epic.org/privacy/wiretap/stats/fisa_stats.html

[131] https://www.cdt.org/files/pdfs/Analysis-Section-215-Patriot-Act.pdf

[132] http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access

[133] http://www.liberty-human-rights.org.uk/materials/introduction-to-ripa-august-2010.pdf

[134] http://ohrh.law.ox.ac.uk/?p=2056

[135] http://ohrh.law.ox.ac.uk/?p=2056 und http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

[136] http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world?INTCMP%3DSRCH

[137] http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[138] http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

[139] http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

[140] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[141] http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthuellt-namen-der-spaehenden-telekomfirmen-1.1736791

[142] http://www.iocco-uk.info/

[143] http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf, Seite 50

[144] http://ipt-uk.com/default.asp

[145] http://www.legislation.gov.uk/ukpga/1994/13/section/10

[146] http://isc.independent.gov.uk/news-archive/17july2013

[147] http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf

[148] http://www.theguardian.com/uk-news/2013/aug/08/privacy-international-challenges-bt-vodafone-gchq

[149] http://www.gesetze-im-internet.de/bndg/BJNR029790990.html

[150] http://www.golem.de/news/datenueberwachung-die-bnd-auslandsaufklaerung-im-rechtsfreien-raum-1309-101324.html

[151] Dr.Berthold Huber, »Die Strategische Rasterfahndung des Bundesnachrichtendiestes – Eingriffsbefugnisse und Regelungsdefizite« Neue Juristische Wochenschrift, 2013, Heft 35, Seite 2576. Siehe auch Punkt 9 der Antwort des Kanzleramts auf eine parlamentarische Anfrage der Linken. Einen Link zu dem Dokument findet man hier: http://www.cr-online.de/blog/2012/05/24/bundesregierung-bestatigt-bnd-prufte-2010-die-nachrichtendienstliche-relevanz-von-37-mio-mails/ Georg Mascolo bringt dieses Argument hier: http://www.faz.net/aktuell/feuilleton/debatten/internationale-datenaffaere-die-aussenwelt-der-innenwelt-12243822.html

[152] http://www.cr-online.de/blog/2013/07/26/nsa-und-bnd-rechtsgrundlagen-gemeinsamkeiten-unterschiede/

[153] http://www.cr-online.de/blog/2013/08/06/warum-die-erhebung-von-metadaten-durch-den-bnd-verfassungswidrig-ist/

[154] http://www.phoenix.de/content//713040

[155] http://www.cr-online.de/blog/2012/02/28/massive-eingriffe-in-grundrechte-bnd-filtert-systematisch-e-mails/

[156] Link zum Bericht: http://dipbt.bundestag.de/dip21/btd/17/086/1708639.pdf

[157] http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf

[158] http://www.cr-online.de/blog/2013/04/04/der-bnd-liest-mit-knapp-3-mio-mails-wurden-2011-kontrolliert/

[159] http://www.sueddeutsche.de/politik/historiker-foschepoth-ueber-us-ueberwachung-die-nsa-darf-in-deutschland-alles-machen-1.1717216

[160] http://www.spiegel.de/politik/deutschland/bnd-und-bfv-setzen-nsa-spaehprogramm-xkeyscore-ein-a-912196.html

[161] http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html

[162] http://www.bundestag.de/bundestag/gremien/g10/

[163] http://www.bfdi.bund.de/cln_029/nn_531474/DE/Themen/InnereSicherheit/Nachrichtendienste/Artikel/Bundesnachrichtendienst.html__nnn=true

[164] http://www.spiegel.de/netzwelt/netzpolitik/nsa-affaere-datenschuetzer-fordern-aufklaerung-von-der-bundesregierung-a-920592.html

[165] *Heumann, S., & Scott, B. (2013). Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany (p.17).,*

http://www.stiftung-nv.de/152069,1031,111427,-1.aspx

[166] *http://www.theguardian.com/commentisfree/2013/sep/13/nsa-behemoth-trampling-rights*

[167] *PRISM: The EU must take steps to protect cloud data from US snoopers; http://www.independent.co.uk/voices/comment/prism-the-eu-must-take-steps-to-protect-cloud-data-from-us-snoopers-8701175.html*

[168] Tagespresse seit dem 06.06.2013; NSA collecting phone records of millions of Verizon customers daily, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order; Sokolow, http://www.heise.de/newsticker/meldung/Big-Data-fuer-Big-Brother-Liest-der-US-Geheimdienst-immer-mit-1884735.html?view=print,.

[169] Tagespresse seit 21.06.2013, Askill/Borger/Hopkins/Davies/Ball, http://www.guardian.co.uk/uk/2013/jun/21/gchq-mastering-the-internet.

[170] Inhaltsaufzeichnung von digitaler Kommunikation, DANA 2/2013, 72; US-Studien warnen vor behördlicher US-Überwachung bei Cloud-Diensten, DANA 1/2013, 26; Millionen Mobilkommunikationsdaten für Ermittlungsbehörden, DANA 3/2012, 128; Schwere Rechtsbrüche des FBI beim Anti-Terror-Kampf, DANA 1/2011, 26; Regierung zu Schadenersatz wegen NSA-Abhörprogramm verurteilt, DANA 1/2011, 29.

[171] Regierung plant massive Ausweitung der Verkehrsdatenüberwachung, DANA 2/2012, 90; Teure Abhörzentrale nimmt Arbeit auf, DANA 4/2003, 28.

[172] Neue Gesetze zur Internetkontrolle, DANA 1/2012, 32; Verlängerung von »USA PATRIOT Act« vorläufig gescheitert, DANA 1/2011, 27; FISA-Berufungsgericht erklärt Abhören ohne Richterbeschluss für legal, DANA 1/2009, 33; Patriot Act bleibt kurzfristig weiter bestehen, DANA 1/2006, 35 (2/2006, 91).

[173] Rauhofer, Die Vorratsdatenspeicherung als Instrument sozialer Kontrolle – eine deutsch-britische Perspektive, DANA 2/2006, 58 f.;

Überwachungsgesetz reißt Löcher in die Privatsphäre, DANA 2/2000, 32.

[174] Poitras/Rosenbach/Schmid/Stark/Stock, Angriff aus Amerika, Der Spiegel 27/2013, 76 ff.

[175] Weichert, Privatheit und Datenschutz im Konflikt zwischen den USA und Europa, RDV 2012, 113 ff.; Korff, Guaranteeing Liberty or Big Brother – Surveillance in the United Kingdom, v. 24.08.2007; https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-korff-surveillance-in-the-united-kingdom-complete.pdf.

[176] Weichert, Big Data und Datenschutz, ZD 2013, 251 ff.

[177] BVerfGE 65, 1 ff. = NJW 1984, 419 ff.

[178] Weichert, Überwachung bringt nichts und macht aggressiv, 2006, https://www.datenschutzzentrum.de/polizei/weichert-ueberwachung2.htm.

[179] Weichert, RDV 2012, 115 ff.

[180] Europapolitiker Brok droht USA mit Aufkündigung wichtiger Abkommen, www.focus.de 27.07.2013.

[181] Konferenz der Datenschutzbeauftragten, PE vom 24.07.2013, Geheimdienste gefährden den Datenverkehr zwischen Deutschland und außereuropäischen Staaten.

[182] Irische Behörde: EU sah 2000 PRISM voraus, www.europe-v-facebook.org 25.07.2013.

[183] Westin, Privacy and Freedom, 1967, 487 S.

[184] Hujer/Neef/Schepp, Finger in der Wunde, Der Spiegel 29/2013, 76 ff.

[185] ULD: Schutz unserer Daten durch Schutz für Edward Snowden, PE 18.07.2013.

[186] Keine Todesstrafe, SZ 27.(28.07.2013, 5.

[187] ULD: PRISM/Tempora – Was wir dagegen tun können, PE 10.07.2013.

[188]http://pib.nic.in/newsite/erelease.aspx?relid=54679

[189]http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights

[190]http://www.outlookindia.com/article.aspx?265192

[191]http://www.deccanherald.com/content/94085/big-brother-smaller-siblings-watching.html

[192]http://www.thehindu.com/opinion/op-ed/indias-cowardly-display-of-servility/article4874219.ece

[193]http://www.thehindu.com/opinion/op-ed/delivering-us-from-surveillance/article5197660.ece

[194]http://forbesindia.com/blog/technology/dear-milind-deora-prakash-javadkar-deserved-the-truth/

[195]http://www.frontline.in/the-nation/indian-help/article4982631.ece

[196]https://www.eff.org/deeplinks/2013/spies-without-borders

[197]https://www.privacynotprism.org.uk/assets/files/privacynotprism/CINDY_COHN-FINAL_WITNESS_STATEMENT.pdf

[198]https://www.eff.org/nsa-spying

[199]http://www.theguardian.com/world/2013/oct/06/sochi-olympic-venues-kremlin-surveillance

[200]http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0

[201]http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[202]https://www.eff.org/deeplinks/2013/09/crucial-unanswered-questions-about-nsa-bullrun-program

[203]https://www.eff.org/deeplinks/2013/10/nsa-making-us-less-safe

[204] Die 13 Prinzipien definieren »*Kommunikationsüberwachung« im modernen Umfeld als Beobachten, Abfangen, Sammeln, Analysieren, Nutzen, Vorhalten und Zurückhalten, Beeinflussen von oder Zugreifen auf Informationen, die vergangene, gegenwärtige oder zukünftige Kommunikation einer Person enthalten, widerspiegeln oder hervorheben. »Kommunikation« beinhaltet Aktivitäten, Interaktionen und Transaktionen, die über elektronische Medien übermittelt werden, wie z.B. Kommunikationsinhalte, Identitäten der Kommunikationsparteien, Standort-Daten wie z.B. IP-Adressen, Zeitpunkt und Dauer der Kommunikation und Informationen der verwendeten Endgeräte.*

[205] https://www.eff.org/deeplinks/2010/11/future-privacy-internet-governance-forum

[206] https://www.eff.org/issues/cell-tracking, http://www.wired.com/threatlevel/2013/03/anonymous-phone-location-data/

[207] https://www.eff.org/deeplinks/2013/01/surveillance-camp-privatize-state-surveillance, https://www.eff.org/deeplinks/2013/09/crucial-unanswered-questions-about-nsa-bullrun-program, https://www.eff.org/deeplinks/2012/04/impending-cybersecurity-power-grab-its-not-just-united-states

[208] https://cippic.ca/en/news/International_Privacy_Principles

[209] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

[210] https://www.eff.org/deeplinks/2013/06/foreign-surveillance-history-privacy-erosions

[211] A Global Reality: Governmental Access to Data in the Cloud

[212] Pub. L. No. 103-414, 108 Stat. 4279

[213] Official Journal C 329, 04/11/1996, 1-6

[214] 47 CFR 42.6

[215] Case C-594/12

[216] 50 USC 1861

[217] 50 USC 1881a

[218] ETS no. 108

[219] Clapper v Amnesty International, Case 11-1025, 2013

[220] Beschwerde Nr. 5029/71

[221] Smith v Maryland, 442 U.S. 735, 1979

[222] Beschwerde Nr. 8691/79

[223] USSID 18

[224] Beschwerden Nr. 30562/04 und 30566/04 §67

[225] Application no. 9248/81

[226] http://www.scl.org/site.aspx?i=ed32980

[227] http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-summer-2011/lessons-wye-river

[228] https://www.commondreams.org/view/2013/05/14

[229] http://www.aclu.org/files/assets/Spyfiles_2_0.pdf

[230] http://www.guardian.co.uk/uk-news/2013/jul/06/home-office-police-childrens-identities-lambert

[231] http://www.sweetliberty.org/issues/privacy/lein1.htm

[232] http://www.networkworld.com/community/blog/cia-wants-spy-you-through-your-appliances

[233] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[234]http://blogs.computerworlduk.com/open-enterprise/2013/06/how-can-any-company-ever-trust-microsoft-again/index.htm

[235]http://www.gnu.org/philosophy/free-sw.html

[236]http://bostonreview.net/forum/protecting-internet-without-wrecking-it/root-problem-software-controlled-its-developer

[237]https://www.commondreams.org/headline/2013/08/23-2

[238]http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html

[239]http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

[240]Als Reaktion auf eine Klage einer Unternehmensgruppe, die sich als »Citizens United« maskiert hat, kam der Oberste Gerichtshof der USA zu dem Schluss, dass Unternehmen Menschenrechte zustehen. Ich unterstütze die Kampagne für eine Verfassungsänderung, die das rückgängig machen will. Siehe http://action.citizen.org/p/dia/action3/common/public/?action_KEY=12266 oder irgendeine bessere Seite.

[241]Vollständiger Lizenztext: https://creativecommons.org/licenses/by-nd/3.0/

[242]https://netzpolitik.org/2013/us-geheimdienst-nsa-der-geheimen-vorratsdatenspeicherung-uberfuhrt/

[243]http://www.cs.princeton.edu/~felten/

[244]http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf

[245]http://www-03.ibm.com/software/products/us/en/analysts-notebook/

[246]https://netzpolitik.org/?s=Analyst%27s+Notebook

[247] https://netzpolitik.org/2012/vorratsdatenspeicherung-visualisiert-was-verbindungsdaten-alles-verraten/

[248] http://www.economist.com/node/16910031

[249] http://213.73.89.124/vds/VDSfinal18.pdf

[250] https://netzpolitik.org/?s=%22big+data%22

[251] http://arxiv.org/abs/1002.0763

[252] http://enriquefrias-martinez.info.p11.hostingprod.com/yahoo_site_admin/assets/docs/mobile-user-models.8193409.pdf

[253] http://fodava.gatech.edu/sites/default/files/FODAVA-12-17.pdf

[254] http://www.research.att.com/~volinsky/papers/portugal.ps

[255] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.42.2517&rep=rep1&type=ps

[256] http://www.aaai.org/Papers/KDD/1998/KDD98-028.pdf

[257] http://www.research.att.com/techdocs/TD_100397.pdf

[258] http://www.ic.unicamp.br/~oliveira/doc/CHI2011-WIP_Towards-a-psychographic-user-model-from-mobile-phone-usage.pdf

[259] *ORF.at; Was Metadaten der NSA verraten; 16. Juli 2013; http://fm4.orf.at/stories/1721492/*

[260] *ORF.at; Wie NSA und GCHQ Verschlüsselung unterminieren; 9. September 2013; http://fm4.orf.at/stories/1724549/*

[261] Unter ‘trusted computing’ verbirgt sich eine von der ‘Trusted Computing Group’ entwickelte Technologie, welche die Kontrolle von Software und Hardware dem Endnutzer entzieht und stattdessen an Drittparteien (z. B. Hersteller) überträgt. Dieses Vorgehen soll der Sicherheit dienlich sein. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie die deutsche Bundesregierung haben

jedoch mehrfach Sicherheits- und verbraucherschutzrechtliche Bedenken gegenüber 'trusted computing' formuliert. Siehe zum Beispiel »Eckpunktepapier der Bundesregierung zu 'Trusted Computing' und 'Secure Boot'" (2012)

...

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/Eckpunktepapier_BregZuTrustedComputingSecureBoot.pdf, zuletzt abgerufen am 3.10.2013, sowie »Stellungnahme des BSI zur aktuellen Berichterstattung zu MS Windows 8 und TPM« (2013), https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Windows_TPM_Pl_21082013.html, zuletzt abgerufen am 3.10.2013

[262] http://heise.de/-189721, zuletzt abgerufen am 3.10.2013

[263] http://www.google.com/glass/terms/, zuletzt abgerufen am 3.10.2013

[264] http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data, zuletzt abgerufen am 3.10.2013

[265] In einer Gesellschaft, in der Computer zunehmend immer mehr Bereiche des Lebens beeinflussen, ist die Frage der Gerätehoheit zugleich eine Frage von Herrschaftsverhältnissen und der Verteilung von Macht. Siehe dazu auch Cory Doctorows vielbeachteten Vortrag auf dem Chaos Communication Congress 28C3 (2011): »The coming war on general computation«, https://www.youtube.com/watch?v=HUEvRyemKSg, zuletzt abgerufen am 03.10.2013

[266] 'Privacy by Design' bezeichnet einen Ansatz, nach dem bereits bei der Entwicklung neuer Technologien der persönliche Datenschutz in die Gesamtkonzeption einzubeziehen, einzuhalten und zu prüfen ist.

[267] Manager Magazin (07/1991), S.156: »Der Pakt mit dem Teufel«

[268] http://fm4.orf.at/stories/1714132/

[269] http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

[270] https://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html

[271] http://fm4.orf.at/stories/1724549/

[272] http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

[273] http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

[274] Internationale Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung; Translation revised by Digitalcourage e.V; ENDGÜLTIGE VERSION 10. JULI 2013; https://de.necessaryandproportionate.org/text

[275] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

[276] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, »Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,« 2009, A/HRC/17/34.

[277] Communications metadata may include information about our identities (subscriber information, device information), interactions (origins and destinations of communications, especially those showing websites visited, books and other materials read, people interacted with, friends, family, acquaintances, searches conducted, resources used), and location (places and times, proximities to others); in sum, metadata provides a window into nearly every action in modern life, our mental states, interests, intentions, and our innermost thoughts.

[278] For example, in the United Kingdom alone, there are now approximately 500,000 requests for communications metadata every year, currently under a self-authorising regime for law enforcement agencies who are able to authorise their own requests for access to information held by service providers. Meanwhile, data provided by Google's Transparency reports shows that requests for user data from the U.S. alone rose from 8888 in 2010 to 12,271 in 2011. In Korea, there were about 6 million subscriber/poster information requests every year and about 30 million requests for other forms of communications metadata every year in 2011-2012, almost of all of which were granted and executed. 2012 data available athttp://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586

[279] See as examples, a review of Sandy Petland's work, 'Reality Mining', in MIT's Technology Review, 2008, available athttp://www2.technologyreview.com/article/409598/tr10-reality-mining/ and also see Alberto Escudero-Pascual and Gus Hosein, 'Questioning lawful access to traffic data', Communications of the ACM, Volume 47 Issue 3, March 2004, pages 77 – 82.

[280] Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 16 2011, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

[281] »People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers ... I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.« United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[282] »Short-term monitoring of a person's movements on public streets accords with expectations of privacy« but »the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.« United States v. Jones, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

[283] »Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts.« U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.)p.562; U.S. v. Jones, 565 U.S. __, (2012), Alito, J., concurring. »Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past...In the Court's opinion, such information, when systematically collected and stored in a file held by

agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention.« (Rotaru v. Romania [2000], ECHR 28341/95, paras. 43-44.

[284] The term »due process« can be used interchangeably with »procedural fairness« and »natural justice«, and is well articulated in the European Convention for Human Rights Article 6(1) and Article 8 of the American Convention on Human Rights.

[285] The UK Interception of Communications Commissioner is an example of such an independent oversight mechanism. The ICO publishes a report that includes some aggregate data but it does not provide sufficient data to scrutinise the types of requests, the extent of each access request, the purpose of the requests, and the scrutiny applied to them. See http://www.iocco-uk.info/sections.asp?sectionID=2&type=top.

[286] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, para 84.

[287] http://www.heise.de/newsticker/meldung/Friedrich-erhebt-Sicherheit-zum-Supergrundrecht-1919309.html

[288] http://www.gesetze-im-internet.de/gg/BJNR000010949.html

[289] http://neusprech.org/brutalstmoegliche-aufklaerung/

[290] http://www.internet-law.de/2013/07/das-supergrundrecht-heist-menschenwurde.html

[291] http://dejure.org/gesetze/GG/1.html

[292] http://de.wikipedia.org/wiki/Grundrecht_auf_Gew%C3%A4hrleistung_der_Vertraulichkeit_und_Integrit%C3%A4t_informationstechnischer_Systeme

[293] https://twitter.com/quirlsen/status/357206271193124864

[294] https://twitter.com/der_skeptiker/status/357393463169388544

[295]https://twitter.com/BiggiPommerin/status/357532477482479617

[296]http://neusprech.org/supergrundrecht/


Hrsg. Markus Beckedahl und Andre Meister
Überwachtes Netz
Edward Snowden und der größte
Überwachungsskandal der Geschichte
new
think
ing
NETZPOLITIK.ORG